# STEALTHY ATTACKS AND DEFENSE STRATEGIES IN COMPETING SENSOR NETWORKS

A Dissertation

by

ALEKSANDRA CZARLINSKA

Submitted to the Office of Graduate Studies of
Texas A&M University
in partial fulfillment of the requirements for the degree of

DOCTOR OF PHILOSOPHY

August 2008

Major Subject: Electrical Engineering

# STEALTHY ATTACKS AND DEFENSE STRATEGIES IN COMPETING SENSOR NETWORKS

A Dissertation

by

ALEKSANDRA CZARLINSKA

Submitted to the Office of Graduate Studies of
Texas A&M University
in partial fulfillment of the requirements for the degree of

DOCTOR OF PHILOSOPHY

Approved by:

| | |
|---|---|
| Chair of Committee, | Deepa Kundur |
| Committee Members, | Karen L. Butler-Purry |
| | Don R. Halverson |
| | Eun Jung Kim |
| Head of Department, | Costas N. Georghiades |

August 2008

Major Subject: Electrical Engineering

# ABSTRACT

Stealthy Attacks and Defense Strategies in Competing Sensor Networks.
(August 2008)

Aleksandra Czarlinska, B.A.Sc., University of Toronto
Chair of Advisory Committee: Dr. Deepa Kundur

The fundamental objective of sensor networks underpinning a variety of applications is the collection of reliable information from the surrounding environment. The correctness of the collected data is especially important in applications involving societal welfare and safety, in which the acquired information may be utilized by end-users for decision-making. The distributed nature of sensor networks and their deployment in unattended and potentially hostile environments, however, renders this collection task challenging for both scalar and visual data.

In this work we propose and address the twin problem of carrying out and defending against a stealthy attack on the information gathered by a sensor network at the physical sensing layer as perpetrated by a competing hostile network. A stealthy attack in this context is an intelligent attempt to disinform a sensor network in a manner that mitigates attack discovery. In comparison with previous sensor network security studies, we explicitly model the attack scenario as an active competition between two networks where difficulties arise from the pervasive nature of the attack, the possibility of tampering during data acquisition prior to encryption, and the lack of prior knowledge regarding the characteristics of the attack.

We examine the problem from the perspective of both the hostile and the legitimate network. The interaction between the networks is modeled as a game where a stealth utility is derived and shown to be consistent for both players in the case of stealthy direct attacks and stealthy cross attacks. Based on the stealth utility, the optimal attack and defense strategies are obtained for each network. For the legitimate network, minimization of the attacker's stealth results in the possibility of attack detection through established paradigms and the ability to mitigate the power of the attack. For the hostile network, maximization of the stealth utility translates into the optimal attack avoidance. This attack avoidance does not require active communication among the hostile nodes but rather relies on a level of coordination which we quantify. We demonstrate the significance and effectiveness of the solution for sensor networks acquiring scalar and multidimensional data such as surveillance sequences and relate the results to existing image sensor networks. Finally we discuss the implications of these results for achieving secure event acquisition in unattended environments.

To My Loving Family

# ACKNOWLEDGMENTS

Foremost I would like to express my gratitude to Dr. Deepa Kundur for her support, advice and encouragement and the experience that she shares with her students. Dr. Kundur is an excellent teacher and a strong supporter of her students, providing them with many opportunities for academic and professional growth.

I would like to thank Professors Karen L. Butler-Purry, Don. R. Halverson and Eun Jung Kim for their participation on my committee, their advice and their valuable teaching. I would also like to thank Dr. Alexander Sprintson and Dr. A. L. Narasimha Reddy for their feedback. Dr. Takis Zourntos has been a source of positivity and I would like to express my gratitude for his perspective and teaching. Special thanks to Dr. Costas N. Georghiades and Dr. Scott Miller for their support and their contributions to a great department for faculty and students.

I would also like to thank my peers in the wireless communications lab for their friendship and advice. Special thanks to William Luh for being a tremendous source of support and friendship.

# TABLE OF CONTENTS

CHAPTER Page

Page

# LIST OF TABLES

# LIST OF FIGURES

FIGURE Page

FIGURE Page

FIGURE Page

# CHAPTER I

# INTRODUCTION

## A. Competing Sensor Networks

Since the early days of the Internet, researchers and users alike have experienced an unprecedented level of connectivity to remote digital information as well as to other distant users. In more recent years, the appeal of connectivity to remote resources has evolved into the fascinating concept of a network capable of reporting information about a distant *physical* environment. This new type of *sensor network* is generally comprised of a large number of networked nodes with sensing, actuation, data processing and communication abilities for the acquisition of scalar or multidimensional data. The wide applicability of sensor networks to the scientific enterprise as well as to industrial and government endeavors is expected to result in the proliferation and ownership of these networks by numerous and often competing entities.

Deployment of a sensor network in a remote environment bestows upon an entity the ability to gather valuable data that may otherwise be unaccessible. To harness the power of such distributed and autonomous acquisition, the data collected by the network must necessarily be reliable and accurate. The authenticity and correctness of the collected data is indeed a core requirement of sensor networks irrespective of the application. This requirement however becomes particularly significant in applications involving societal welfare and safety, as well as in systems where the acquired information is utilized by an end-user for critical decision-making.

In this work we propose and address the twin problem of carrying out and defending against a stealthy attack on the information gathered by a sensor network. A

The journal model is *IEEE Transactions on Automatic Control.*

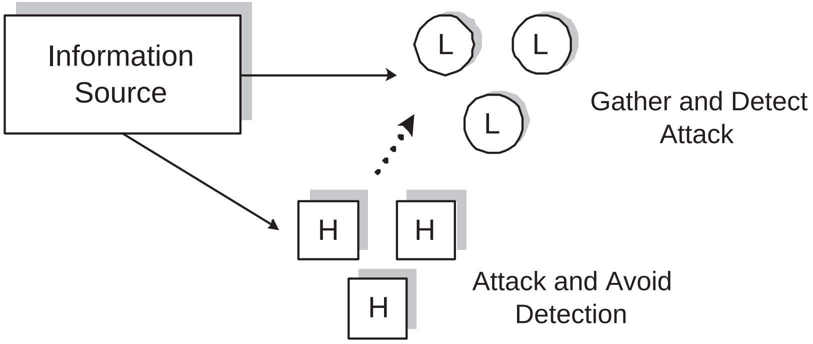


Fig. 1. Dual stealthy attack and defense problem.

stealthy attack in this context is an intelligent attempt to disinform a sensor network in a manner that minimizes the chance of the attack being uncovered. In response, a stealthy attack detection mechanism is an approach to maximize the chance of detecting the attack and to mitigate its impact on the accuracy of the collected data. In examining this mirror problem, we refer to the entities that perpetrate the attack as hostile (H) and label the entities defending against the attack as legitimate (L) as shown in Figure 1.

In investigating this novel problem, we introduce the framework of two competing networks and thus extend the notion of a sensor network attacker. Prior considerations restricted the attacker to a single entity that injects false data into a network by physically capturing a *small* subset of nodes or breaking their encryption keys to render them malicious [1]. The current formulation enables the study of a potentially large set of distributed hostile nodes that form an allied network. Such distributed hostile nodes cause disinformation at the legitimate sensors by interfering with their local readings in a manner that preserves the hostile nodes' stealth. This form of distributed denial of service on sensing is also referred to as an actuation attack to emphasize its active nature and occurrence at the sensing level prior to encryption.

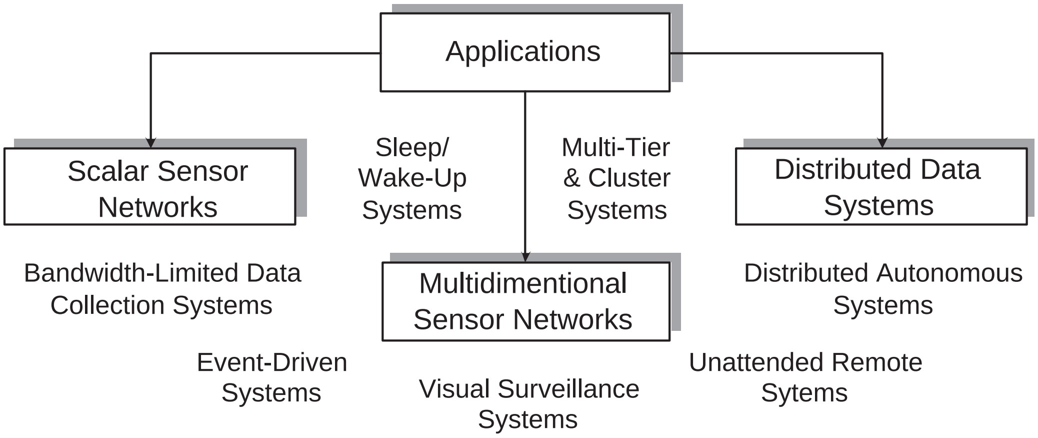

Applications
Scalar Sensor Networks
Sleep/ Wake-Up Systems
Multi-Tier & Cluster Systems
Distributed Data Systems
Bandwidth-Limited Data Collection Systems
Multidimentional Sensor Networks
Distributed Autonomous Systems
Event-Driven Systems
Visual Surveillance Systems
Unattended Remote Sytems

Fig. 2. Applications of the stealthy attack mechanism and the dual attack defense mechanisms.

By attacking at the sensing level, a hostile opponent thus gains entrance into an information gathering system for the purposes of manipulation.

The mitigation and detection of stealthy sensor network attacks is thus of interest to entities that wish to gather information in the presence of competitors. This arises in the case of both scalar and image networks deployed over large and potentially hostile areas to detect an event of interest in the environment such as the passing of an object or an individual. A stealthy attack in this case can result in an event of interest being unnoticed with potentially significant consequences. As shown in Figure 2, defense mechanisms against stealthy attacks are also required for information gathering systems that rely on sleep/wake-up cycles, event triggers or multi-tier architectures [2]. In such systems, stealthy attacks can falsely trigger or mistrigger the network to drain its limited energy reserves and misinform the network regarding the presence or absence of an event. Defense mechanisms against these attacks are thus beneficial for systems that must be reliable, autonomous and distributed (RAD) while operating in physically exposed or accessible environments.

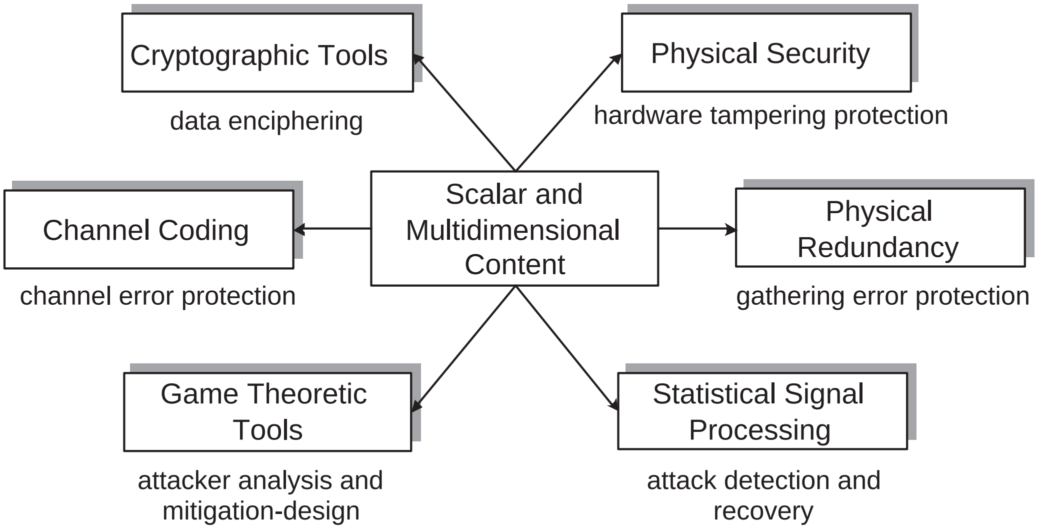

Cryptographic Tools
data enciphering
Physical Security
hardware tampering protection
Channel Coding
channel error protection
Scalar and Multidimensional Content
Physical Redundancy
gathering error protection
Game Theoretic Tools
attacker analysis and mitigation-design
Statistical Signal Processing
attack detection and recovery

Fig. 3. Approaches for secure collection (our focus) and dissemination of sensor data.

Currently the primary defense mechanisms for the secure collection and dissemination of sensor data are chiefly based on cryptographic tools and associated protocols, as well as on the use of sensor redundancy with sufficiently dense deployments. Cryptographic techniques tailored to the low power and computation paradigm of sensor networks are especially vital for safeguarding the data during its wireless transit towards the sink. Redundancy with topology control helps to achieve the desired physical coverage and also mitigate the effects of sporadic sensor errors due to faults or harsh environmental conditions. Other complimentary approaches include physically secure sensor hardware to prevent tampering and key extraction, signal processing approaches for trust monitoring and coding theory approaches to protect against transmission errors.

In the case of competing networks however, these techniques alone no longer guarantee the authenticity, integrity and availability of the collected sensor data. In particular, the distributed nature and actuation abilities of the hostile nodes enable them to inject false readings into arbitrarily many sensors prior to the encryption stage. Attack detection and mitigation in this scenario are further complicated by the lack of a priori knowledge regarding the attacker's strategies. In contrast with systems containing noise disturbances, attack parameters cannot generally be obtained or estimated from the system. Indeed an organized attacker wishing to disinform a data collection network may judiciously select and vary the attack parameters to avoid detection and to maintain stealth. To address the stealthy attack problem, we thus propose the use of game theoretic analysis to characterize the optimal strategies of the attacker under various attack models. Such characterization enables the design of detection and mitigation strategies based on statistical signal processing and sensor redundancy as shown in Figure 3. Thus to secure sensor data, we expand the array of toolsets to ensure that the information is protected not only during its transit but also during the collection process.

### B. Contributions

In this work we present the novel problem of securing sensor data for the case of competing sensor networks. We explicitly consider the interplay between the two networks in terms of attack and defense strategies. This is achieved via a dual framework that addresses the problem from the perspectives of both networks. From the perspective of the hostile network, we present strategies to carry out an attack that is stealthy and minimizes the chance of detection. From the perspective of the defending network, we present strategies that maximize attack detection and also mitigate the attack.

The main contribution to sensor network security is a framework for analyzing attacks that may be widespread and carried out in an informed manner. This is in contrast with existing models which assume that attacks are limited to a small number of nodes and that the attacker's exposure is limited specifically through this small-scale injection and the use of stolen cryptographic materials. As part of the framework, we develop a stealth condition for the attacker and apply it to various attack models. We show that use of game theoretic tools is possible in this problem to obtain meaningful information regarding the active attack and that it facilitates the use of established statistical signal processing tools. We demonstrate the importance of this problem to scalar and image-acquiring sensor networks and show the effectiveness of the proposed solution techniques.

The main difficulties of the proposed problem stem from the distributed nature of the attacker, the possibility of tampering during the sensing process prior to encryption, and a lack of estimates for the attack parameters in contrast with the conventional case of disturbances due to noise. We overcome these challenges for scalar and multidimensional sensor networks for the following three cases of inter-network competition.

1. Stealthy Direct Competition. We formulate the stealthy direct competition problem where each hostile node may attack one legitimate node in a one-to-one attack. We develop a stealth condition metric and show its consistency and relevance for both networks in terms of attack mitigation and detection such as through the Neyman-Pearson paradigm. We show how the concept of Nash equilibria allows the hostile network to determine the optimal attack parameter based on the stealth condition without knowing the defense actions of the legitimate network. This optimal attack parameter for each hostile node allows the H network as a whole to minimize the chance of being detected. This attack avoidance does not require active communication among the hostile

nodes but rather a level of coordination which we quantify. For the hostile network H, the direct stealthy attack yields a favorable level of stealth $\mathcal{S}$, power of attack $P_a$ and power-communication-detection $PCD$ metric compared with other stealth approaches. We thus show how the stealth condition metric allows the hostile network to perpetrate the attack in a distributed manner. The main result for H is the ability to determine a specific value of the attack parameter without the knowledge of the legitimate network defense.

For the legitimate network L, we employ the developed stealth condition to determine the optimal defense strategies. This analysis has implications for the selection of a local sensor decision threshold as well as for the number of sensor nodes in the legitimate network. Importantly, we show how the defense strategies can be selected without knowledge of the attack parameter utilized by H. We demonstrate how attack analysis enables use of an optimal detector based on the Neyman-Pearson approach and show its effectiveness in detecting and mitigating the attack. Based on these results we discuss the role of forward and feedback encryption between L and the sink in ensuring secure data collection.

2. Stealthy Cross Competition. We formulate the stealthy cross competition problem where each hostile node H may attack more than one neighboring legitimate node. Importantly two hostile nodes H may attack the same neighboring legitimate L node for a two-to-one cross attack. At the conceptual level for H, this problem resembles cross interference which is typically undesirable. We develop the stealth condition for this case of attack and determine the optimal attack parameters for each hostile node. Surprisingly we show that there exist strategies for the cross attack that achieve superior stealth for H than the direct attack without the need for hostile node communication. Finally we discuss im-

plications for the common knowledge that must be possessed by each hostile node in order to satisfy the game theoretic equilibria for attack stealth.

For the legitimate network, we employ the derived stealth condition to obtain the best defense strategies. We show how the cross attack presents a greater challenge for L than the direct attack in terms of attack detection in the Neyman-Pearson paradigm. We show that both the optimal and sub-optimal detectors in the cross attack benefit from analysis of the optimal strategies of H. Importantly we show that the optimal detection and mitigation strategies obtained for the stealthy direct attack apply to the stealthy cross attack and are thus consistent.

3. Stealthy Image Network Competition. We formulate the stealthy image network competition where the hostile network H wishes to disinform and mistrigger a legitimate network L that consists of both (scalar) sensors and camera nodes capturing potentially valuable visual content. The hostile network may utilize a direct or a cross attack strategy to misguide the sensors. The legitimate network may rely on a combination of detection and mitigation strategies developed for the direct and cross attacks, as well as on image processing techniques at the camera nodes.

   For the legitimate network, the inclusion of image processing introduces a new source of information but also a new source of variability in the decision making process. This variability is a result of varying (outdoor) conditions and of the image processing limitations caused by restricted camera resources. We show how a desired event acquisition performance can be achieved at the camera nodes despite these limitations and the presence of stealthy attacks. We demonstrate the performance of the solution using surveillance sequences and relate it to existing prototype image networks. Finally we discuss the implications of these results for achieving secure event acquisition in unattended environments.

## C. Organization

This work focuses on the competition between two sensor networks in the context of sensor data security. To reflect this framework, the chapters are organized in terms of an increasing level of attack difficulty and correspondingly more challenging defense solutions. Chapter II provides the background literature as well as the models and measures that are critical to the competing sensor networks problem. Chapter III presents the direct stealthy attack and defense solutions with its implications for scalar data networks. Chapter IV presents the cross stealthy attack and defense strategies for scalar data networks and its implications for hostile sensor deployment. Chapter V presents the attack and defense strategies for multidimensional sensor networks that collect visual surveillance data. Finally Chapter VI summarizes our findings and discusses future work.

# CHAPTER II

# PRELIMINARIES

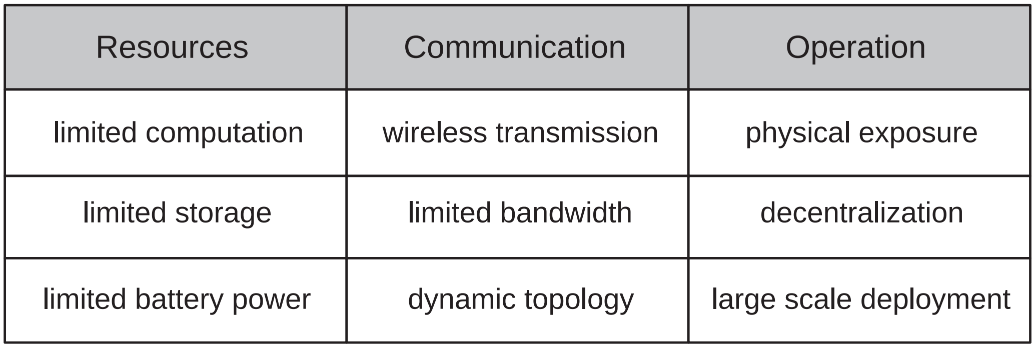
## A. Characteristics of Sensor Networks for Data Acquisition

In this work we consider two competing sensor networks co-deployed in a common environment with opposing goals regarding the secure collection of data. To explore this problem, we begin with a brief overview of the general characteristics and challenges of sensor networks as they pertain to reliable and secure data gathering.

Sensor networks are comprised of a collection of sensor nodes for scalar or multidimensional data gathering. Such data may include sensor readings regarding the ambient conditions or the presence, absence or change in observed motion, temperature, magnetic activity, acoustic activity, seismic activity, toxin levels, as well as visual information regarding a target of interest [3]–[11].[1] Sensor nodes also possess storage, processing, communication and actuation capabilities to facilitate and enable the collection and transmission of sensor data to a sink such as an intermediate cluster head or a base station.

Despite these capabilities, the data collection and dissemination process in sensor networks is made challenging by the nodes' resource limitations as overviewed in Figure 4. Achieving the level of data reliability required by an application thus necessitates the design of algorithms and technologies that are tailored to the low cost-power-computation paradigm [14], [15]. These designs often favor the use of sensor redundancy in lieu of expensive hardware or algorithms to attain the desired data

[1] Though typically envisioned for ground applications, sensor nodes have also been developed for aerial [12], [13] and aquatic applications. The latter was originally prototyped in a much larger version during the cold war for the detection of foreign submarines.



| Resources | Communication | Operation |
|---|---|---|
| limited computation | wireless transmission | physical exposure |
| limited storage | limited bandwidth | decentralization |
| limited battery power | dynamic topology | large scale deployment |

Fig. 4. General challenges in sensor networks.

collection and dissemination performance. Furthermore, sensor networks that are required to remain operational for long periods of time in unattended environments often employ sleep/wake-up, trigger-based and multi-tier methodologies [16], [17]. In such approaches, only a few sensors remain awake during any period of time and trigger the other sensors within a cluster or within a higher tier when a potential event has been detected. Such approaches have shown significant potential in real-world prototype testbeds [7], [3], [16] in applications ranging from intelligent infrastructure monitoring and target tracking to image-based distributed surveillance.

In the case of scalar sensor nodes, further economy in the data collection and dissemination process is often achieved by requiring the sensors to make local decisions about events in the environment instead of transmitting raw sensor data to the sink (with the noteworthy exception of scientific applications that require the precise phenomena readings) [18]. Indeed it has been shown that under many power and bandwidth constraints, such strategies are asymptotically optimal for the detection of events [19], [20]. In the case of multidimensional sensor networks, this economical approach often translates into the use of lightweight image processing techniques for the collection and transmission of lower resolution images to the end-user unless otherwise requested [7], [21], [22].

In addition to resource limitations, the deployment of sensors in physically accessible, unattended and potentially hostile environments presents further challenges for reliable data collection and dissemination as shown in Figure 4. Gaps in sensing coverage may result if nodes in a certain area become depleted or suffer a fault [23]–[25]. This situation is typically remedied through dense deployments and coverage repair such as through limited mobility [26]–[29]. Sensing fidelity may also be compromised due to the presence of an attacker. The attacker may physically capture a subset of the nodes and their encryption keys to render the nodes malicious and inject false readings into the network. In such cases, node re-keying and redundancy, as well as tamper-proof hardware may be utilized [30]. The latter approach however may be too expensive for certain applications where nodes need to be low-cost and potentially disposable. Node redundancy and re-keying on the other hand may not protect against a distributed hostile network attacking at the physical level of sensing or the physical layer of communication. The latter attack belongs to a broader category of attacks referred to as (distributed) denial of service attacks with a rich literature of defenses [31]–[34]. The former is referred to as a distributed denial on sensing and is the focus of this work [35], [36].

In summary, to achieve reliable data collection and distribution, sensor network design must overcome the numerous resource limitations, communication challenges and operational challenges outlined in Figure 4. While some of these challenges are also present in other networks, it is the simultaneous presence of all these issues in sensor networks that distinguishes them from other networks. These challenges also in part characterize the type of vulnerabilities that may be exploited by opponents if no defense mechanisms are in place.

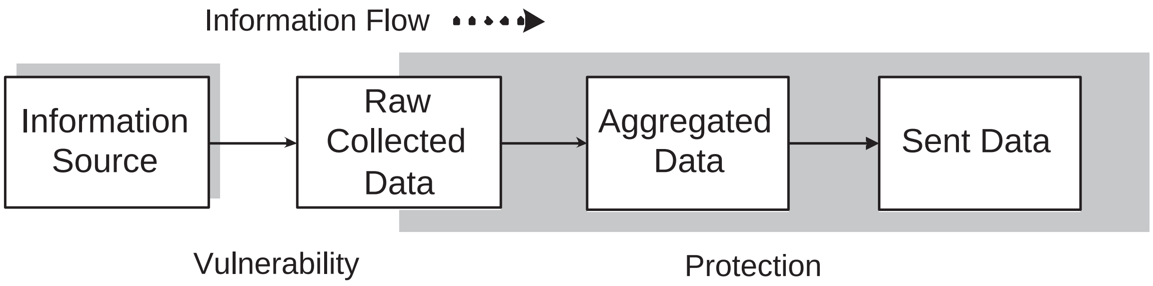


Fig. 5. Information flow during the sensor data collection and dissemination process showing protected and vulnerable parts of the process.

### B. The Secure Data Acquisition and Stealthy Attack Problems

In this work we investigate the data *collection* process at the physical layer in the case of competing networks deployed in a common environment. In comparison with previous studies, we focus on attacks that occur during the data gathering process prior to encryption and prior to the data's travel through the network towards the sink as shown in Figure 5.

For this case of competing networks, we extend the attacker model to that of a distributed hostile network. This is in contrast with previous studies that focused on a small number of captured nodes that are subverted to behave maliciously within the legitimate network. This competing network scenario is shown in Figure 6. The legitimate nodes L and the hostile nodes H are deployed in a common environment where they collect readings regarding a source of interest. The L nodes wish to determine if an event of interest has occurred in the environment based on readings obtained from the source. The decision of each L node may be utilized directly for network applications. It may also be considered collectively with the decisions of other L nodes at a cluster head as shown in Figure 6. Both approaches have proven of particular interest to trigger-based applications and tracking based applications

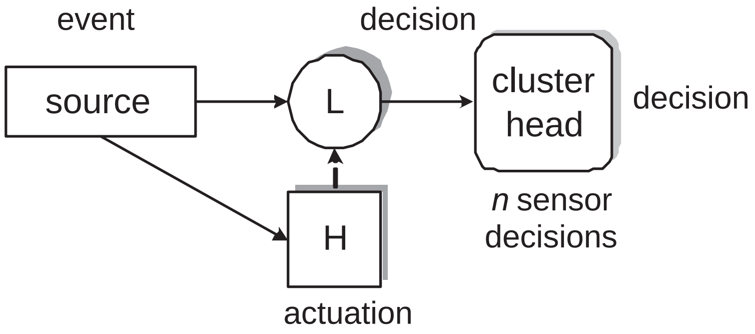


Fig. 6. Data gathering in the competing networks scenario.

that operate in large or unattended areas over prolonged periods of time. In such applications, the individual sensors and/or the cluster head trigger a set of higher-tier nodes such as cameras [3], [7], [16].

Based on its deployment in the environment, a hostile node may utilize actuation to disrupt the readings collected by a legitimate node L. The actuation may be performed using a variety of methods depending on the underlying sensor technology and the application (Appendix C). Land-based actuation for example includes magnetometer, acoustic, laser and mobility based technologies while aquatic versions include sonar and diffusion-based technologies. The effect of the actuation is a perturbation of the readings collected by a legitimate node L such that an incorrect decision regarding the presence or absence of an event may be made by the node. Based on the distributed nature of the attacker, each L sensor may be affected with some non-zero probability. Thus node redundancy without attack detection may not be sufficient to avoid incorrect sensor and collective decisions. In the competing networks scenario shown in Figure 6, the goals of each network are thus as follows:

- Goals of the Legitimate Network. The legitimate network wishes to collect both individual and collective sensor decisions that are correct regarding the presence or absence of an event. In the case of an attack, the legitimate network wishes to maximize the chance of uncovering the attack at the cluster head.

- Goals of the Hostile Network. The hostile network wishes to cause as many incorrect individual sensor decisions as possible among the $n$ sensors in a cluster. The hostile network H also wishes to cause an incorrect collective decision at the cluster while minimizing the chance of the attack being uncovered. The hostile network thus wishes to select attack strategies that are stealthy.

## C. System Models and Metrics

In this section we expand on the goals of each network by presenting the associated models and measures utilized to evaluate the success of each network in this competitive scenario.

### 1. Competing Sensor Networks Model

To study the twin problem of stealthy attacks and defense strategies for the gathering of sensor network data, we model the competition between the two networks for sensing fidelity as a static game. The static game model enables study of situations where one player's outcome depends not only on his/her actions, but also on the choices of the other players. This is crucial in the competing networks scenario where the hostile nodes' optimal attack parameters depend on the legitimate nodes' defense strategies and vice versa.

A static game $\mathcal{G}$ consists of a triplet $\langle \Gamma, A, U \rangle$ that specifies the game. $\Gamma$ is the set of players $\Gamma = \{1, ..., k, ..., n\}$ in the game and $A = \{A_1, ..., A_k, ..., A_n\}$ where $A_k$ is the set of actions available to player $k$. $U = \{u_1, ..., u_k, ..., u_n\}$ where $u_k$ is the utility for player $k$ and specifies player $k$'s preferences for every action profile of the game.

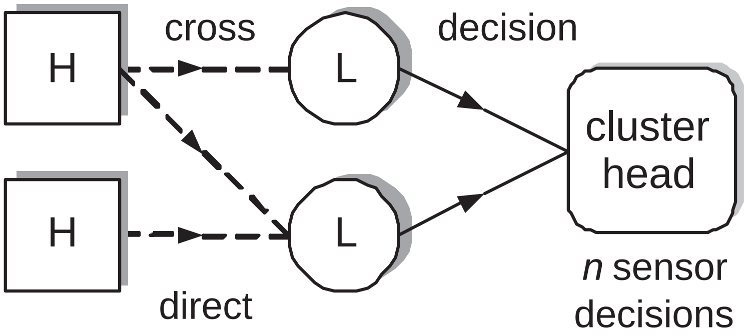


Fig. 7. Based on deployment and goals, a hostile node H may attack one or more or none of its neighboring legitimate nodes L. This abstraction depicts a subset of two hostile nodes with the possibility of cross-attack.

In modeling $\mathcal{G}$, we must thus specify the players, the action set of each player and the associated utilities as they pertain to the secure data acquisition and stealthy attack problem.

The general model of the secure data acquisition and stealthy attack problem is depicted in Figure 7. Based on its deployment and goals, each hostile node may attack one or more (or none) of the legitimate nodes. As shown in Figure 7, the direct attack which is examined in Chapter III refers to the case of one hostile node attacking one legitimate node with some probability. The cross attack which is examined in Chapter IV refers to one hostile node attacking more than one legitimate node with the possibility of cross-over among hostile nodes. In this context, an attack strategy for hostile node $h_i$ from its set of possible actions $A_{hi}$ is a probability of attacking a given legitimate node based on the direct or cross attack model.

For the legitimate network, each sensor makes a decision regarding the presence or absence of an event in the environment as shown in Figure 7. This process of data acquisition at each sensor is modeled via Eq. (3.1), where $o_i$ is an observation made by sensor $i$ regarding the source $O$ and $\gamma_i$ is the mapping used by sensor $i$ to produce the decision $x_i \in \{0, 1\}$ regarding the presence or absence of the event. Each sensor makes the decision by comparing its reading to a threshold $T_{h_i}$, where $\mathbb{I}_P$ is an indicator function which is equal to 1 if $P$ is true and is equal to 0 otherwise. Based on the probability density function $f_{0_i}$ of the observation $o_i$, a sensor reports an even with probability $p_i$.

$$x_i = \gamma_i(o_i) = \mathbb{I}_{\{o_i \geq Th_i\}} \quad \text{s.t} \quad p_i = \int_{Th_i}^{\infty} f_{0_i}(\alpha) d\alpha \tag{2.1}$$

In the context of energy-constrained sensor networks, this data acquisition model plays an important role. In the works of [20], [37]–[39] for instance, the distributed detection of phenomena via sensor networks is explored. One of the general conclusions is that for networks with channel bandwidth and power constraints, a large number of sensors with binary decisions is asymptotically optimal [20]. That is, increasing node redundancy produces a better result than obtaining more detailed information from each sensor. Specifically, the binary sensor setup is not generally asymptotically optimal for arbitrary sensor correlations and distributions $f_{0_i}$, but rather it is optimal for the *i.i.d* Gaussian or exponential case. It is noted however that in practice the simplicity of using binary decisions may outweigh the small gain in bit performance achieved by using more complicated schemes. Thus in this work we assume that each sensor utilizes the same threshold $T_h$ and that the readings are *i.i.d.* This results in a probability $p$ that a sensor registers an event.

Based on the data acquisition and attack models, the hostile network wishes to maximize the probability of an undetected attack while the legitimate network wishes to minimize this probability. From the perspective of a game $\mathcal{G}$, any utility can be used to represent the preferences of each player as long as it represents these preferences in a consistent manner [40]. This signifies that if a player prefers action $a_1$ to action $a_2$

and action $a_2$ to action $a_3$, then he/she must prefer action $a_1$ over action $a_3$ and the utility must preserve this consistency[2]. For the stealthy attack and defense game, we develop a utility referred to as the stealth condition $\mathcal{S}$ and show that it is consistent for both H and L in terms of attack detection (such as through the Neyman-Pearson detection paradigm). Based on the stealth condition $\mathcal{S}$, the optimal action $a_k^*$ of each player $k$ is determined where $a_k^* \in A_k : \mathcal{S}_k(a_k^*, a_{-k}) \geq \mathcal{S}_k(a'_k, a_{-k}) \quad \forall a'_k \in A_k$ where the notation $-k$ denotes all the players other than player $k$. The optimal actions of the players in $\mathcal{G}$ reveal the best attack and defense approaches for the case of competing sensor networks.

### 2. Performance Metrics

In investigating the competing sensor networks problem, we examine the data collection process from the perspective of the hostile network and from the perspective of the legitimate network. The success of each network in competing with the other is thus examined in terms of that network's specific goals from Section B. We now briefly re-state the goals of each network and present the measures of success for each.

The goal of the hostile network H is to disinform and misguide the legitimate network during the data gathering process. To this effect, H wishes to cause as many incorrect individual sensor decisions among the $n$ sensors within a cluster as possible. H also wishes to cause an error in the collaborative decision at the cluster head while minimizing the chance of attack detection. From the perspective of H, the following measures are thus of relevance in the stealthy attack problem.

[2] Strictly, given a set of actions $A$ and a consequence function $g : A \rightarrow C$ that maps $A$ to the set $C$ of possible consequences, all we require is a preference relation (a complete transitive reflexive binary relation) $\succeq$ on the set C. However we may use a utility function $u : C \rightarrow \mathbb{R}$ which defines the preference relation $a \succeq b$ by the condition $u(a) \geq u(b)$.

1. Power $P_a$ of the attack. This is the number of sensors among the $n$ sensors in the cluster that report an incorrect decision (a 1 instead of a 0, or vice versa) as a result of the attack. From the attacker's point of view, $P_a \in \{0, n\}$ should be as large as possible (subject to the condition that the attack stealth is maximized). The power of the attack thus measures the number of incorrect individual decisions that H is able to cause.

2. Stealth $S$ of the attack. The *relative* stealth of one attack strategy over another is measured through the stealth condition $\mathcal{S}$. Alternatively, the *absolute* stealth of an attack strategy is measured through the pair $P_D$-$P_{FA}$, where $P_D$ is the probability of detecting the attack at the cluster head and $P_{FA}$ is the probability of raising a false alarm about the attack. From the point of view of H in the Neyman-Pearson paradigm for instance, $P_D$ should ideally be small for a given $P_{FA}$ in order to evade detection.

3. Power-Communication-Detection $PCD$ of the attack. Instead of measuring the power $P_a$ and the stealth $S$ of the attack individually, a joint measure can be considered given that both $P_a$ and $S$ are simultaneously important to the attacker. Furthermore, such a joint measure facilitates comparisons among attacks. Of particular interest in the stealth scenario is a comparison of the number of communications required among the hostile nodes to coordinate the stealthy attack. Thus we generalize the joint comparison measure to include the concept of inter-node communication $C$. In this context, $PCD = P_a/(C \cdot S)$. More precisely, $PCD$ is given by Eq. (2.2).

$$PCD = \frac{\text{No. attacked nodes}}{(1 + \text{No. communications}) \cdot (1 + P_D)} \tag{2.2}$$

The definition of $PCD$ offsets each of the denominator terms by 1 to account for cases where $C = 0$ and/or $P_D = 0$. As can be seen from Eq. (2.2), it is beneficial for the hostile network to increase the number of affected sensors while maintaining a low level of inter-node communication and a small probability of attack detection.

For the legitimate network, the goal is to collect as many correct individual sensor and collective decisions as possible while maximizing the chance of attack detection. Thus the legitimate network L is interested in the following measures of success:

1. Power $P_d$ of the defense. The power of the defense is the number of sensors among the $n$ sensors in the cluster that report a correct decision (a 1 given that an event occurred, and a 0 given that no event occurred) in the presence of an attack. Thus the power of the defense is the complement of the power of the attack where $P_d = n - P_a$. From the defense's point of view, $P_a \in \{0, \ldots, n\}$ should be as small as possible (subject to the condition that the attack stealth is minimized). The power of the defense thus measures the number of correct individual decisions that L gathers from the source in the presence of attack.

2. Stealth $S$ of the attack. Based on the competition between the two networks for stealth and detection, the absolute stealth of an attack strategy from the point of view of L is also measured through the pair $P_D$-$P_{FA}$. From the point of view of L in the Neyman-Pearson paradigm for instance, $P_D$ should ideally be as large as possible for a given $P_{FA}$ in order to detect the attack.

3. Redundancy $R$ of the defense. The redundancy $R$ of the defense is the number of sensors $n$ required within a cluster to minimize the stealth $S$ while achieve a given power of defense $P_d$. From the perspective of $L$, the requisite level of

sensor redundancy $R \geq 1$ should be small enough to limit unnecessarily dense deployments while achieving detection goals.

In the sensor network scenario, a variety of other measures can be utilized to track a network's performance such as the energy consumption and the lifetime of the network (defined variously depending on the application). Such measures are commonly utilized to study the performance of individual networks in ad hoc and harsh environments. In this work we wish to focus exclusively on the previously unexplored concept of sensor network competition. As such we focus on metrics that assess the level of success in this competition as defined in this section. Importantly, the fundamental metrics defined in this work might be combined with specific experimental or theoretical energy consumption models to derive other valuable information in the context of competition.

### D. Literature Review and Classification

This work examines the competition between two sensor networks one of which is hostile with the intent of disinforming the second network regarding events of interest in the environment. From the legitimate network's perspective, the central focus of this work is thus the development of mechanisms for the secure *collection* of sensor data in the case of competition. From the hostile network's perspective, the focus of this work is on perpetrating an attack that successfully disinforms the network. In relating this work to existing sensor network research, we thus examine the relationship from both the attack and defense perspectives. Appendix C provides a somewhat orthogonal overview of other fields of relevance to sensor networks such as coverage, deployment and actuation.

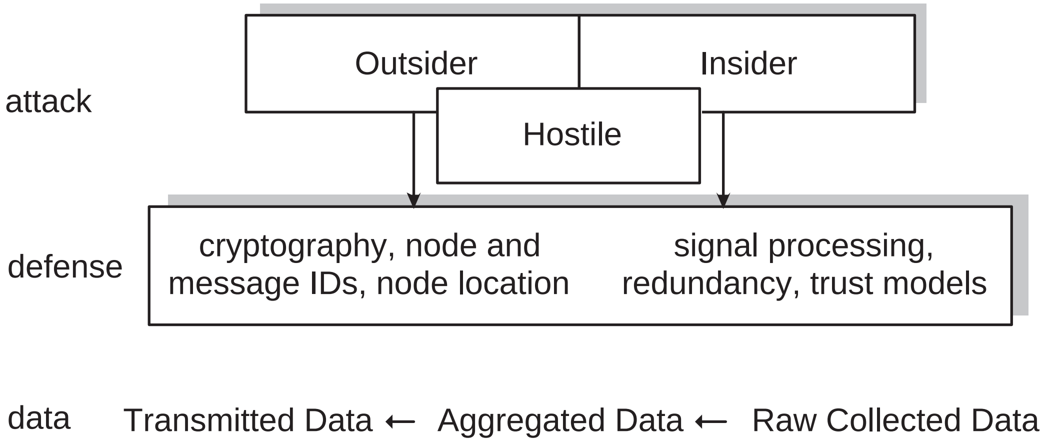

attack
Outsider
Insider
Hostile
defense
cryptography, node and message IDs, node location
signal processing, redundancy, trust models
data
Transmitted Data ⟵ Aggregated Data ⟵ Raw Collected Data

Fig. 8. Classification of the stealthy hostile attack with respect to existing work in terms of attack, defense and affected data.

### 1. Relationship of Literature to Our Work

The competing sensor networks problem as it relates to existing research is depicted in Figure 8 where the relationship is initially shown broadly in terms of attacks, defenses and affected data.

As shown in Figure 8, sensor network attacks are often subdivided into the categories of insider and outsider attacks depending on whether the attacker has possession of secret keys belonging to the legitimate network. Interestingly, the stealthy attack perpetrated by a distributed hostile network appears to straddle these two traditional categories by exhibiting characteristics of both. In the new attack, the hostile opponent does not have "insider" access to the legitimate network's secret keys thus qualifying as an outsider attack. On the other hand, the attack enables the injection of false data into the legitimate network as though the attacker had by-passed the network's encryption, thus qualifying as an insider attack. This latter feature is made possible by the attack occurring at the vulnerable physical layer of sensing as depicted in Figure 5. Finally we make an important observation regarding the distributed hostile attack. We note that use of cryptography at the sensors typically forces an attacker to physically compromise nodes to obtain keying information. Given the distribution of the legitimate sensors over an area, the procurement of a given number of keys may be too laborious for the attacker and thus imposes limits on the degree of possible compromise. In the hostile attack, this restriction no longer applies given the distributed nature of the attacker and the physical layer at which the attack is perpetrated. Figure 9 depicts a finer-grained comparison of the new attack with existing attacks in terms of their effect of the network and its data. The hostile attack is listed both under the physical attacks category as a DDoS (distributed denial on sensing) and as an attack on data. The arrow in Figure 9 illustrates that attacking the network at one layer may facilitate attacks on other layers. For instance, a Sybil attack may be carried out first such that the "Sybil node" has several supposedly valid identities that it uses to communicate with the rest of the network. In such a scenario the extra identities of the node can collude to report false data. In other words, the Sybil attack allows one compromised node to have greater impact on the aggregation result [15]. The attacker may also skew the aggregation result by first carrying out a Denial of Service (DoS) attack. In this scenario the blocked nodes are not reporting their local values and are hence excluded from the overall aggregation [32].

The competing sensor networks scenario is also compared to existing schemes in terms of defense strategies as shown in Figure 8. In the context of sensor networks, it is typically assumed that to perpetrate an insider attack an opponent must compromise secret keys. It is thus assumed that only a small number of nodes and keys will be compromised [41]–[45]. Typical defense mechanisms against insider attacks therefore include the use of sensor redundancy, signal processing schemes (such as data

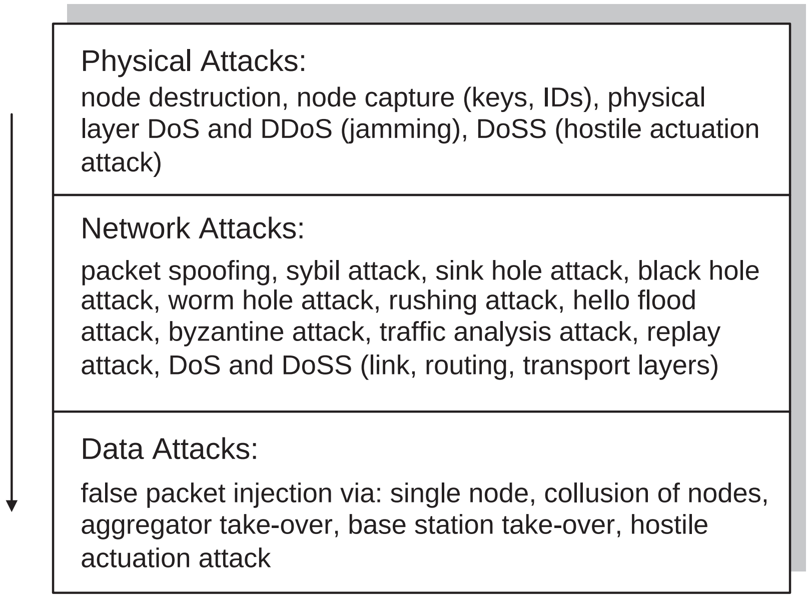

Physical Attacks:
node destruction, node capture (keys, IDs), physical layer DoS and DDoS (jamming), DoSS (hostile actuation attack)
Network Attacks:
packet spoofing, sybil attack, sink hole attack, black hole attack, worm hole attack, rushing attack, hello flood attack, byzantine attack, traffic analysis attack, replay attack, DoS and DoSS (link, routing, transport layers)
Data Attacks:
false packet injection via: single node, collusion of nodes, aggregator take-over, base station take-over, hostile actuation attack

Fig. 9. Classification of the stealthy hostile attack with respect to existing attacks based on their effect on the network and its data.

aggregation) and the use of trust models [46], [47]. In the case of a hostile distributed network however, node redundancy along with data aggregation are no longer sufficient due to the number of affected nodes at the sensing level. Therefore as shown in Figure 3, in this work we consider defense mechanisms against the hostile attack that are based on a combination of attack analysis (through game theory), statistical signal processing (through attack detection) and sensor redundancy [48]–[51].

Sensor network attacks may also be considered in terms of the data that they affect as shown in Figure 8. Due to its occurrence at the physical layer of sensing, the new hostile attack affects the raw collected data and therefore the aggregated data that is derived from it. The attack does affect data during its transmit through the network. An interesting observation is that the new attack may also be viewed as one that compromises multiple security goals simultaneously. Figure 10 shows that the

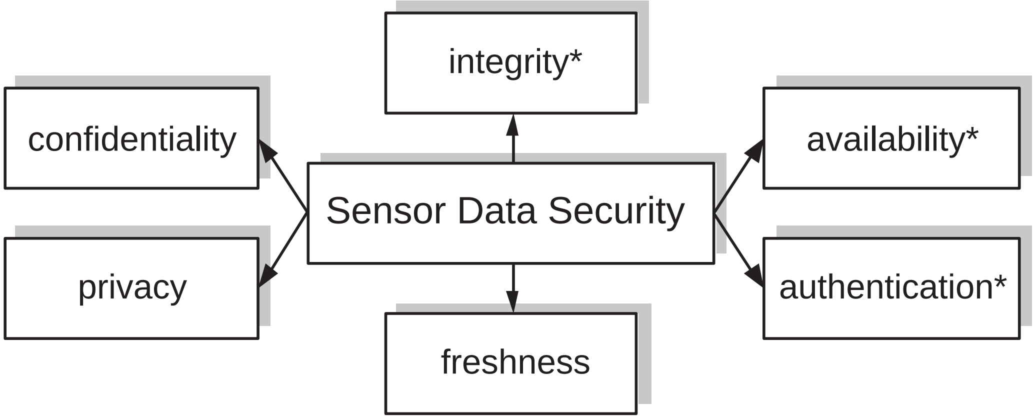


Fig. 10. Sensor network security goals affected by the hostile attack (*).

attack compromises the sensor data integrity by altering the collected measurements. With a slight stretch of the traditional definition, we may also conclude that the attack compromises data authentication since the measurements do not purely originate from the source as expected. Furthermore the hostile attack affects data availability since characteristics of the source are no longer available to the end-user.

### 2. Game Approach to Sensor Network Security

The theory of games has been used extensively in the study of problems with multiple cooperative or non-cooperative players where the preferences of each player in the game can be defined consistently [52]. The model of a game is utilized in situations where the outcome experienced by a player depends not only on his/her own actions but also on the unknown actions of others. Game theory may be viewed as a form of "optimization of an entity's actions" given that all problem variables are not centralized at the entity but rather distributed among several entities [53], [54]. Importantly, though many problems can be modeled as a game or optimization, such modeling need not always yield a tractable formulation or a meaningful solution [55], [56].

In this work we focus on two-player, non-cooperative, zero-sum, static games and show that the models yield meaningful solutions for both the hostile and the legitimate networks. Generally, a two-player game is non-cooperative if each player attempts to achieve his/her own goals (which may or may not conflict with the goals of the other players) and where there is no mechanism to enforce contracts (cooperation) between the players. Games in which players can enforce contracts through outside parties are termed cooperative games [40], [57]. The game is said to be zero-sum if the sum of the payoffs of the two players must always add to zero. Hence if player one wins a payoff of 4 units, player two must loose 4 units. A game is said to be static if both players make a move simultaneously without knowing a priori what their opponent is choosing. A static game is only played once (one move per player) but can be extended by repeated play. An important concept in non-cooperative static games is that of a (pure or mixed) Nash equilibrium point (at least one such point is guaranteed to exist). A Nash equilibrium point is simply a "solution" to the game predicting the players' moves (assuming the players are always rational and choose the highest payoff possible). The equilibrium occurs when neither player has any payoff incentive to deviate from the strategy if their opponent does not deviate from it (i.e. deviating from this strategy will not increase the payoff unless the other player changes his/her moves) [40].

In recent years game theoretic approaches to various aspects of sensor network security have been presented. In [58] the authors describe how to disrupt the coverage of an opponent's network by modeling node removal as a two-stage game. In [59] the authors model secure key distribution schemes in a probabilistic way. They show how the game theoretic model can be formally translated into properties that would render the distribution schemes more secure. In [60] the authors employ game theory to study medium access control. Using this approach they provide a protocol that achieves short-term fairness within a window size of 3-4 packets per node, in comparison with existing MAC protocols which require 80-140 packets per node to achieve fairness. In [61] the authors adapt existing game theoretic approaches to the particular challenges associated with secure routing in sensor networks. Specifically, the authors develop a game theoretic model that accounts for non-simultaneous decision making and incorporates history information into the decision making process. In [62] the authors develop an analytical model of data-centric information routing in sensor networks under the constraints of trading off individual node energy versus the overall network's goals. These recent advances demonstrate the potential of game theoretic modeling for sensor network security analysis and design.

## 3. Data Content Security in Sensor Networks

The body of literature on sensor network security is vast, with numerous attack models and proposed solutions. Attack countermeasures exist at various network levels and are aimed at protecting the data during various stages of the collection, processing and distribution process. This section overviews a subset of the specific attacks shown in Figure 9 along with their mitigation strategies. We focus the discussion on the subset of attacks most directly related to our proposed work at the physical sensing layer as shown in Figure 9. As such, we focus the review on attacks that affect the collection of data such as through denial of service (DoS) attacks, trust model violations and a special attack referred to as the "Byzantine Generals' Problem." We also examine tampering at the physical layer such as through node capture, and attacks on the node processing level such as during the aggregation process.

### a. Attacks on Collection and Processing

In [63], sensor decision redundancy allows the fusion center to select the correct hypothesis regarding a source within some probability while channel coding protects against the binary decisions being flipped during transmission. This methodology however does not protect against a hostile attack where sensor errors may not be rare but pervasive throughout the network and where the attack hypotheses are not known. Due to the large amount of information collected by sensors, it is often necessary and useful to perform data aggregation [64]–[66]. However if the aggregation function is performed by a designated subset of nodes that become compromised by an attacker, then the resulting data may be misleading [67].

Compromising a single aggregator is often sufficient to skew the data from dozens or hundreds of nodes. In [68], [69] the authors propose a statistical en-route filtering mechanisms that relies on the assumption that multiple neighboring nodes witness the same original event and can confirm this event by using MACs along the path from the aggregator to the base station. Any packet that fails any of the MAC tests is discarded. In [70], the authors describe LEAP+. The proposed Localized Encryption and Authentication Protocol is a key management protocol for sensor networks that is designed to support in-network processing. The protocol restricts the security impact of a node compromise to the immediate network neighborhood of the compromised node. In [71] the authors propose an SQL like language called TAG (Tiny Aggregation Service). In this approach the base station generates queries. The sensors then route data back to the base station according to a routing tree. At each point in the tree, data is aggregated according to the routing tree and the aggregation function demanded by the query.

In [72] the authors propose mechanisms that enable more complex aggregation functions to be computed approximately and prove strict guarantees on the approximation of the queries. In [73] the author analyzes the robustness of various aggregation functions to the capture of $k$ nodes (with $k \ll N$ where $N$ is the total number of nodes). It is concluded that most functions are not robust to such tampering with the exception of the count statistic and of any other statistic meeting the proposed $(k, \alpha)$ definition of functions. In [44] the authors present a three-stage technique called aggregate-commit-prove to protect against false data injection at $k \ll N$ nodes as well as a take over of the aggregator. To achieve this the authors make use of Merkle hash-trees and interactive proofs. In [74] the authors propose a secure aggregation technique that protects against at most 1 compromised node. Their approach borrows the $\mu$TESLA protocol for symmetric key management to generate and validate the MACs of individual nodes for multihop message authentication. Most recently, in [75] the authors extend the methodology found in [44] to include a hierarchy of aggregators (several aggregators send data to a higher level aggregator that aggregates their result). Their approach guarantees that the attacker does not gain more by attacking the intermediate aggregators than he/she would by compromising the individual nodes that report to the aggregators.

### b. Physical Attacks

The category of physical attacks encompasses activities where a malicious entity tampers with the physical components and hardware of the node. Physical attacks pose a large threat to sensor networks due to their unattended operation in open and possibly hostile environments. One way of coping with this attack is to tamper-proof the node's physical package or hardware [76]–[78]. Since sensors need to be low-cost and numerous, the extra cost of such hardware may be prohibitive [32], [76].

In [79] the authors introduce the concept of a secure localization scheme called the ECHO protocol to prevent attackers from eavesdropping the physical location of sensor nodes. Their work relies on the physical properties of sound and RF signal propagation. In [80] the authors introduce the use of directional antennas to defend against wormhole attacks. As such they propose “turning the table” on the attackers by using physical characteristics of the sensor network *against* the attackers. In [81] the authors study the modeling and defense of sensor networks against search-based physical attacks where an opponent walks through the sensor field with signal detecting equipment. Their solution strategy relies on a subset of nodes detecting the attack and transmitting this warning to other nodes. The nodes that detect such an attack or receive such a warning shut off their power and hence become undetectable.

### c. Denial of Service Attacks

A Denial of Service (DoS) attack in sensor networks and networks in general is defined as any event that diminishes or eliminates the network’s capacity to perform its expected function [32], [34]. DoS attacks in sensor networks may be carried out at the physical, link, routing and transport layers. At the physical layer an attacker may simply jam a sensor’s radio transmissions, either constantly or intermittently [32]. Solutions to this attack include spread spectrum communications, priority messages, lower duty cycling, and node mobility. To attack at the link layer an attacker may simply intentionally violate a communication protocol, attempting to cause collisions. Solutions to this level of attack include error-correction codes, rate limitation and small frames. At the routing layer a malicious node may take advantage of a multihop network by refusing to route messages. Protection mechanisms at this layer include encryption, egress filtering, authorization monitoring and redundancy. Finally at the transport layer a DoS may consist of packet flooding which drains resources. At this layer solutions include issuing client puzzles and using authentication mechanisms. In [82] the authors present an efficient mechanism called message-specific puzzle to mitigate DoS attacks for broadcast authentication. In addition to signature-based or $\mu$-Tesla-based authentication, the approach adds a weak authenticator in each broadcast packet which is computationally difficult for an attacker to forge. In [83] the authors employ cooperative game theory between the nodes of the legitimate network. This game between the legitimate sensor nodes is based on three factors: cooperation, reputation and quality of security. Nodes form clusters with other nodes that have similar payoff functions. Misbehaving nodes that drop traffic may thus be detected. In [84] the authors formulate the attack-defense problem as a two-player, nonzero-sum, non-cooperative game between an attacker and a sensor network. Using this formulation they propose two schemes for preventing DoS attacks. The first approach is Utility based Dynamic Source Routing (UDSR). It incorporates the total utility of each route in data packets, where utility is a value that the legitimate network is trying to maximize. The second approach is based on a watch-list, where each node earns a rating from its neighbors based on its previous cooperation in the network.

### d. Trust Models

Given the likelihood of sensor node compromise in a sensor network, the associated trust model cannot blindly include all network nodes. In [85] the authors propose a trust evaluation scheme where nodes evaluate other nodes based on factors such as experience statistics, data value, intrusion detection results and references from other nodes. In [86] the authors describe a probabilistic solution based on a distributed trust model with an initial secret dealer. In [87] the authors propose a reputation-based framework for high integrity in sensor networks.

### e. Byzantine Generals' Problem

The original version of the Byzantine Generals' Problem is presented in [88]. The Byzantine Generals Problem involves a group of generals, each commanding a division of the Byzantine army. In its simplest form, each general independently makes a one bit binary decision to attack (bit 1) or to retreat (bit 0) based on his/her local observations of the enemy. Importantly, we require that all the generals agree on a *common* decision to attack or retreat (their combined resources are required in order to succeed should they choose to attack). To achieve this consensus, each general sends his/her decision to every other general. Each general then makes his/her final decision based on applying a majority rule to the incoming decisions.

The difficulty of this original formulation stems from the fact that some of the generals are allowed to be corrupt. This means that they are allowed to recommend bad strategies (recommend 1 when 0 should have been recommended and vice versa) *and* furthermore, they are allowed to recommend different strategies to different generals. In other words, a corrupt general may recommend decision bit 1 to one of its neighbors and decision bit 0 to another neighbor. The corrupt generals hence behave not only erroneously but also inconsistently. It has been shown that the Byzantine Generals' Problem can be reduced to a "Commander and Lieutenants" problem [88]. If message authentication (encryption) is allowed, then it is possible in many cases to reach a consensus when an arbitrary number of traitorous generals is present. If message authentication is not available, in general we can only protect the system if the number of traitors is less than a third of the total number of generals [89].

As extended to general systems, a Byzantine fault is one in which a component of some system not only behaves erroneously, but also fails to behave consistently when interacting with multiple other components. For instance, a sensor node taken over by an attacker may report a certain decision about its environment to one neighbor (for instance it transmits "enemy present"), but sends a different message to another neighbor ("enemy absent") [90]. Correctly functioning components of a Byzantine fault tolerant system will be able to reach the same group decisions regardless of Byzantine faulty components [91]. It is also insightful to examine the connection between the Byzantine Generals' Problem and the stealthy hostile attack model. In the original form of the Byzantine Generals' Problem, we require that all non-corrupt generals reach a consensus in the presence of a number of corrupt generals that send erroneous and inconsistent decisions. If we have access to message authentication then under many situations we are able to achieve Byzantine fault tolerance in the presence of an arbitrary number of corrupt generals [88].

In contrast with this setup, in the stealthy attack problem we do not require that all the sensor nodes reach a consensus. Rather, only one select entity (the cluster head) is required to reach a *correct* decision about the presence or absence of an attacker. The connection between the two problems may be better understood with the following analogy. In the stealth attack formulation, each sensor may be thought of as a general. Each general makes a local decision about the presence or absence of an event. However, *each* general also has his/her own *advisor* (the hostile node that interferes with the readings). Each advisor may be corrupt with some probability and change the general's decision. Once the general finalizes his/her local decision based on his/her observation and the advisor's input, the decision is sent to an overall commander (the cluster head) through encrypted means. Hence the decisions (messages) cannot be forged during the communication process. It is the commander (the cluster head) that ultimately decides whether *at least* one general has sent an incorrect decision under the influence of a hostile advisor but the commander does not know *which* generals may have been ill-advised by a hostile advisor.

# CHAPTER III

# STEALTHY DIRECT COMPETITION*

## A. Introduction and Motivation

In this chapter we wish to investigate the competing sensor networks scenario for the case of a direct stealthy attack. In a direct stealthy attack, each hostile node may attack a legitimate node with some probability, causing an incorrect decision at the sensor. Unlike occasional errors, decision errors due to a distributed stealthy attack may be persistent over time and pervasive throughout the cluster. Such errors can corrupt the data acquisition process and cause misinformation regarding events of interest in the environment.

We examine the problem from the perspective of both the hostile and the legitimate network. The interaction between the networks is modeled as a game where a stealth utility is derived and shown to be consistent for both players. Based on the stealth utility, the optimal attack and defense strategies are obtained for each network. For the legitimate network, minimization of the attacker's stealth results in the possibility of attack detection through the Neyman-Pearson paradigm and the capability of mitigating the power $P_a$ of the attack. For the hostile network, maximization of the stealth utility translates into the optimal attack avoidance. This attack avoidance does not require active communication among the hostile nodes but rather a level of coordination which we quantify. The direct stealthy attack yields a favorable level of stealth $\mathcal{S}$, power of attack $P_a$ and power-communication-detection

*Part of the material in this chapter is reprinted with permission from A. Czarlinska and D. Kundur, "Event-Detection in Wireless Visual Sensor Networks through Scalar Collaboration and Game Theoretic Consideration," *IEEE Transactions on Multimedia, Special Issue on Multimedia Applications in Mobile/Wireless Contexts*, August 2008, to appear. © 2008 IEEE.

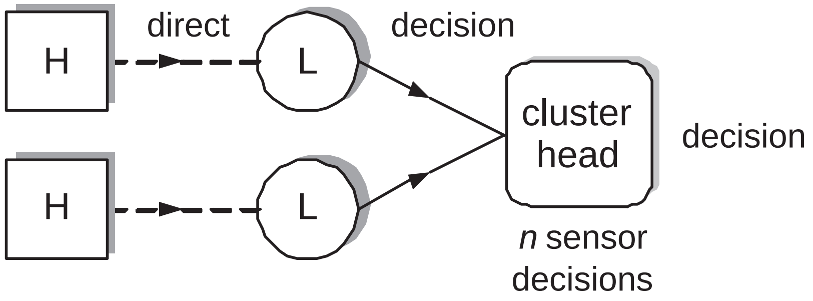


Fig. 11. Direct stealthy attack model.

$PCD$ compared with other stealth approaches.

### B. System Model

We consider a legitimate network L and a hostile network H deployed in a common environment by competing entities. Based on deployment and goals, each hostile node may attack a legitimate node with some probability in a direct "one-to-one" attack as shown in Figure 11.

A legitimate node $l_i$ where $i \in \{1, \ldots, n\}$ obtains an observation $o_i$ from the environment regarding the source of interest $O$. Each node utilizes a local decision threshold $T_h$ to decide whether an event of interest has occurred in the environment based on Eq. (3.1) where $f_0$ is the probability density function of the source $O$ and $x_i$ is the realization of a decision made by node $i$. This scenario is depicted in Figure 12a. The decision of each node can thus be modeled as a Bernoulli random variable $X_i$ as given by Eq. (3.2).

$$x_i = \gamma_{(}o_i) = \mathbb{I}_{\{o_i \geq Th\}} \quad \text{s.t} \quad p = \int_{Th}^{\infty} f_0(\alpha) d\alpha \tag{3.1}$$

$$X_i = \begin{cases} 1 & \text{w.p. } p \\ 0 & \text{w.p. } 1-p \end{cases} \tag{3.2}$$

Each hostile node $h_i$ where $i \in \{1, \ldots, n\}$ performs local actuation $y_i$ upon a legitimate node with a probability $0 \leq q \leq 1$ as shown in Figure 12b. Based on this binary symmetric error model, a hostile node may interfere with the local readings of a sensor with probability $q$ such that an incorrect decision is made. Importantly in the case of attack, the probability $q$ may take on *any* value based on the actions of the attacker and is thus generally unknown. This is in contrast with decision errors caused by occasional sensor faults where the value of $q$ is generally known through quality testing and is typically assumed to be small. The actuation attack of node $h_i$ can thus be modeled as a Bernoulli random variable $Y_i$ as given by Eq. (3.3) where the *effect* of the attack is given by Eq. (3.4) where $\oplus$ denotes modulo 2 addition and corresponds to the binary symmetric error model of Figure 12b. Thus as shown in Figure 12b, the decision of a legitimate sensor node $l_i$ under the attack model is given by a Bernoulli random variable $Z_i$ as given by Eq. (3.5).

$$Y_i = \begin{cases} 1 & \text{w.p. } q \\ 0 & \text{w.p. } 1-q \end{cases} \tag{3.3}$$

$$Z_i \quad = X_i \oplus Y_i \tag{3.4}$$

$$Z_i = \begin{cases} 1 & \text{w.p. } r \\ 0 & \text{w.p. } 1-r \quad \text{where} \quad r = q + p - 2pq \end{cases} \tag{3.5}$$

Importantly in the general case without constraints, the attack probability $q$ may take on any value in the permissible range. In the scenario of competing networks however, this is no longer the case. In particular, the legitimate network employs redundancy in the form of $n$ sensor decisions that are sent to the cluster head as shown

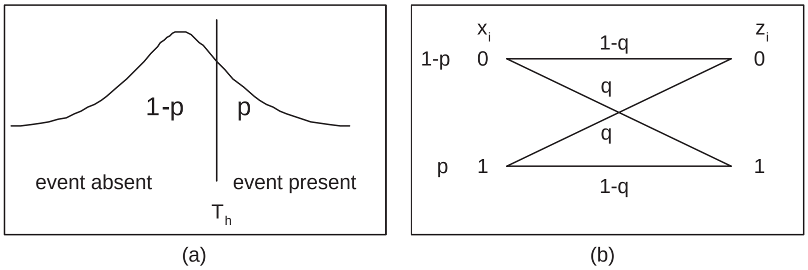


Fig. 12. (a) Binary sensor model with sensing threshold $T_h$ and resulting probability of witnessing an event $0 \leq p \leq 1$. (b) Basic bit error model due to fault or unstealthy attack where $0 \leq q \leq 1$ is typically small for faults but may be arbitrarily large for unstealthy attacks.

in Figure 11. A *competing* hostile network must therefore select attack strategies that are informed and competitive in this scenario rather than arbitrary. Specifically H faces a situation where under no attack, the cluster head receives a vector $\mathbf{x}$ of $n$ sensor decisions where each decision comes from a distribution $Bern(p)$. To achieve stealth and minimize the probability of attack detection, the hostile network wishes to attack such that the attacked vector $\mathbf{z}$ from distribution $Bern(r)$ statistically resembles the prestine vector $\mathbf{x}$. The attacker thus wishes to satisfy the stealth condition $\mathcal{S}$ given in Definition 1.

**Definition 1** *The stealth condition $\mathcal{S}$ of the hostile sensor network H for the direct attack is given by Eq. (3.6) where $w$ is the weight of a vector which is the number of 1's contained in the vector and defined as $w(\xi) \doteq \sum_{i=1}^{n} \xi_i$ for a vector $\xi$ of length $n$.*

$$\mathcal{S} = Pr\{w(\mathbf{Z}_{pq}) = w(\mathbf{X}_p)\} \tag{3.6}$$

We now provide the intuition behind the stealth condition and formally show its consistency and effectiveness for the attacker in Section C. Informally, the stealth condition allows the hostile network to flip individual sensor readings (from 1 to 0 and vice versa) to achieve a power of attack $P_a$ while maintaining the appearance of a statistically legitimate decision vector as received by the cluster head on average. By altering individual sensor decisions within the stealth constraint, H can also cause the cluster head to make the wrong collective decision about an event. The cluster head typically requires that a specified number of sensors $c$ report an event before deciding that an event has most likely occurred [3], [7], [92]. The requisite number of sensors $c$ (also known as the "weight" [6] or the degree of aggregation DoA [3]) may be determined experimentally, approximated based on expectations or obtained via detection mechanisms such as based on the Neyman-Pearson paradigm (Section D). For instance to perform an approximation, if there are $n$ sensors and each sensor has a probability $p$ of witnessing an event (based on its threshold $T_h$), then the average expected number of sensors that report an event is $c \approx np \pm \epsilon$ where $\epsilon$ may be determined experimentally. In this context, the stealth condition $\mathcal{S}$ as defined in Eq. (3.6) is a more general and strict condition on the attack such that the attacker is able to minimize the chance of detection at the cluster head without knowledge of the specific cluster head mechanism.

Thus in the game between the two networks, the attacker wishes to choose an optimal value of attack parameter $q^*$ such that the weight of the attacked data (which depends on probabilities $p$ and $q$) generally matches (in terms of the probability of occurrence) the weight of the unaltered data (which depends on the probability $p$ alone). In general the attacker need not know the probability $p$ since the sensor threshold $T_h$ may not be known to the attacker. In that case the selection of the attack parameter is performed through game theoretic optimization where the sensors with unknown parameter $p$ are treated as an opponent and where the attacker is treated as the other player with unknown parameter $q$. The direct stealthy game $\mathcal{G}$ between H and L is thus given formally by definition 2.

**Definition 2** *The direct stealthy game is given by:*

$$\mathcal{G} = \langle \Gamma, A, U \rangle = \langle \{L, H\}, \{A_1, A_2\}, \{u_1, u_2\} \rangle \tag{3.7}$$

$$A_1 = \{p : p \in [0,1]\} \quad A_2 = \{q : q \in [0,1]\} \tag{3.8}$$

$$u_1(p,q) = 1 - Pr\{w(\mathbf{X}_p) = w(\mathbf{Z}_{pq})\}, u_2(p,q) = Pr\{w(\mathbf{X}_p) = w(\mathbf{Z}_{pq})\} \tag{3.9}$$

To solve the game and obtain the optimal actions of each player, we are looking for best response functions [1] $B_1(q^*)$ and $B_2(p^*)$ where the notation $B_a(b)$ denotes the best response $B$ of player $a$ to the opponents best strategy $b$ as given by Eqs. (4.21) and (4.22) respectively.

$$B_1(q^*) = \text{arg min} \quad {}_{0 \leq p \leq 1} \quad Pr\{w(\mathbf{X}_p) = w(\mathbf{Z}_{pq})\} \tag{3.10}$$

$$B_2(p^*) = \text{arg max} \quad {}_{0 \leq q \leq 1} \quad Pr\{w(\mathbf{X}_p) = w(\mathbf{Z}_{pq})\} \tag{3.11}$$

C. Stealthy Attack Results

In this section we analyze and solve the direct stealthy attack game $\mathcal{G}$ from definition 2. We begin by deriving the stealth condition $\mathcal{S}$ from Eq. (3.6) through Problem 1 which we also refer to as the overlap problem.

**Problem 1 (OVERLAP)**

*GIVEN:* $w(\mathbf{X}) \sim Binomial(n,p)$

$w(\mathbf{Y}) \sim Binomial(n,q)$

*FIND:* $\mathcal{S} = Pr\{w(\mathbf{X}) = w(\mathbf{X} \oplus \mathbf{Y})\}$.

A more general relaxed version of the stealth condition that allows the attacker to deviate from the optimal weight by a factor of $\epsilon$ is derived via Problem 2.

[1] In general the best response can be a functional [56].

**Problem 2 (OVERLAP-2)**

*GIVEN:* $\epsilon$ *a fixed integer*

$$w(\mathbf{X}) \sim Binomial(n, p)$$

$$w(\mathbf{Y}) \sim Binomial(n, q)$$

*FIND:* $\mathcal{S}' = Pr\{|w(\mathbf{X}) - w(\mathbf{X} \oplus \mathbf{Y})| \leq \epsilon\}$.

Problem 3 focuses specifically on the best strategies of the attacker and finally Problem 4 presents the solution to the entire game including the strategies of the legitimate network L.

**Problem 3 (OPTIMAL-q)**

*GIVEN:* $w(\mathbf{X}) \sim Binomial(n, p)$,

$w(\mathbf{Y}) \sim Binomial(n, q)$

*FIND:* $\arg\max_{q \in [0,1]} Pr\{w(\mathbf{X}) = w(\mathbf{X} \oplus \mathbf{Y})\}$.

**Problem 4 (STATIC-GAME)**

*GIVEN:* $w(\mathbf{X}) \sim Binomial(n, p)$,

$w(\mathbf{Y}) \sim Binomial(n, q)$

*FIND:* $B_1(q^*)$ *and* $B_2(p^*)$ *from Eqs. (4.21) and (4.22).*

In addressing the problems in this chapter, we make use of the following notation. We make extensive use of the binomial coefficient $\binom{a}{b}$ where $\binom{a}{b} = a!/(b!(a-b)!)$ for a positive integer $a$ and non-negative integer $b \leq a$, and 0 otherwise (negative and fractional $a$ and $b$, defined using Gamma functions, have no physical meaning in our problem) [93]. Here the factorial of $a$, written as $a!$ is equal to $a \times (a-1) \times (a-2) \times \cdots \times 2 \times 1$. We also use the notation $x \downarrow 0$ to indicate the limit from above, or more intuitively, $x$ approaching 0 from the right-side. The absolute value $|\cdot|$ when applied to a finite set, denotes the cardinality of that set, while when applied to non-sets it denotes the real absolute value as will be clear from the context.

### 1. Attack Analysis

First we set out to solve Problem 1 also referred to as the overlap problem. The aim of Lemma 1 is to outline the necessary and sufficient condition of the legitimate and attacker's bit vectors overlapping, such that $\mathbf{x} \oplus \mathbf{y}$ has the same weight as the pristine $\mathbf{x}$. The goal is to first determine the weight of $\mathbf{x} \oplus \mathbf{y}$, which is illustrated in Figure 13. The idea is that whenever the 1s in $\mathbf{x}$ and $\mathbf{y}$ do not overlap, these positions contribute to the overall weight of $\mathbf{x} \oplus \mathbf{y}$, since $1 \oplus 0 = 0 \oplus 1 = 1$.

**Lemma 1** $w(\mathbf{x}) = w(\mathbf{x} \oplus \mathbf{y})$ *if and only if the number of* $1$*s in* $\mathbf{x}$ *and* $\mathbf{y}$ *coincide in exactly* $m = w(\mathbf{y})/2$ *positions.*

**Proof 1** *Let* $k = w(\mathbf{x})$, $l = w(\mathbf{y})$, *and let* $A$ *be the set of positions in* $\mathbf{x}$ *that have a value of* $1$, *i.e.* $A = \{i : x_i = 1\}$ *and let* $B$ *be the set of positions in* $\mathbf{y}$ *that have a value of* $1$, *i.e.* $B = \{i : y_i = 1\}$. *Then* $k = |A|$ *and* $l = |B|$. *The set of positions in both* $A$ *and* $B$ *that coincide is* $A \cap B$ *so by definition* $m = |A \cap B|$. *The set of positions that do not coincide is* $(A \cup B) - (A \cap B)$. *In binary addition, bits that match always add to* $0$, *and bits that do not match always add to* $1$, *hence* $w(\mathbf{x} \oplus \mathbf{y}) = |(A \cup B) - (A \cap B)| \overset{(a)}{=} |(A \cup B)| - |(A \cap B)| \overset{(b)}{=} |A| + |B| - 2|A \cap B| = k + l - 2m$, *where* $(a)$ *results because* $A \cap B \subset A \cup B$, *and* $(b)$ *follows from the principle of inclusion and exclusion. If* $w(\mathbf{x}) = w(\mathbf{x} \oplus \mathbf{y})$, *then* $k = k + l - 2m$, *which implies* $m = 1/2$. *Conversely, if* $m = 1/2$, *then* $w(\mathbf{x} \oplus \mathbf{y}) = k + l - 2(1/2) = k = w(\mathbf{x})$.

**Lemma 2** *Suppose* $\mathbf{x}$ *and* $\mathbf{y}$ *have exactly* $m$ *overlapping* $1$*s. Then* $w(\mathbf{x}) \geq m$ *and* $w(\mathbf{y}) \geq m$ *must satisfy:*

$$n - w(\mathbf{x}) \geq w(\mathbf{y}) - m \tag{3.12}$$

**Proof 2** *Define* $k$, $l$, $A$, *and* $B$ *as in the proof of Lemma 1. The distinct* $1$*-positions over both* $\mathbf{x}$ *and* $\mathbf{y}$ *are given by the set* $A \cup B$. *Since the total number of distinct*

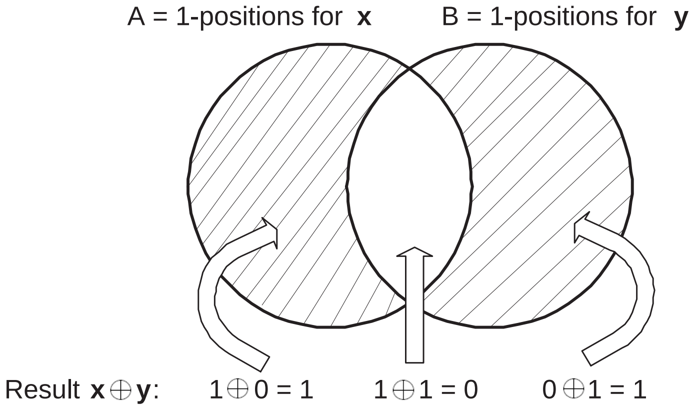


Fig. 13. Visualization of Lemma 1: when 1-positions do not overlap (intersect) the result is a bit 1, otherwise a bit 0.

*1-positions cannot exceed $n$ (for either $\mathbf{x}$ or $\mathbf{y}$ would be of length greater than $n$), we have $n \geq |A \cup B| = |A| + |B| - |A \cap B| = k + l - m$.*

The following definition is based on Lemma 2 and will be used in subsequent proofs.

**Definition 3** *Given a number $m$, the pair $(k, l)$ is said to be* well-defined *if it satisfies $n - k \geq l - m$, and $n \geq k \geq m$, $n \geq l \geq m$.*

In Lemma 3 we look at the conditional probability of $\mathbf{x}$ and $\mathbf{y}$ overlapping in exactly $m$ positions. The technique used in the proof is to fix one of the vectors, i.e. $\mathbf{x}$, as shown in Figure 14, and then choose $\mathbf{y}$s so that only $m$ of their 1s overlap with any of the $\mathbf{x}$'s 1s. This probability turns out to be a hypergeometric distribution.

**Lemma 3** *Let $E$ be the event that the number of 1s in $\mathbf{X}$ and $\mathbf{Y}$ overlap in exactly $m$ positions. Then*

$$Pr(E|\{w(\mathbf{X}) = k \text{ and } w(\mathbf{Y}) = l\}) = \frac{\binom{k}{m}\binom{n-k}{l-m}}{\binom{n}{l}} \quad (3.13)$$

$$= \frac{\binom{l}{m}\binom{n-l}{k-m}}{\binom{n}{k}} \quad (3.14)$$

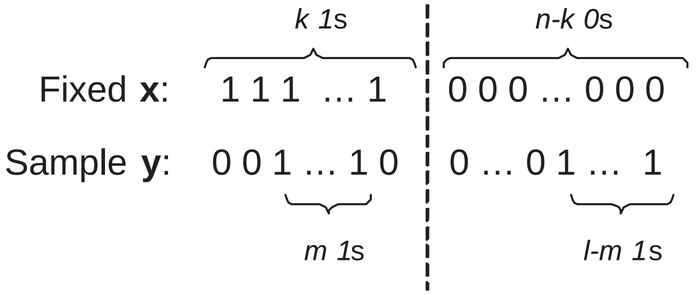


Fig. 14. Visualization of Lemma 3: choosing exactly $m$ of $\mathbf{y}$'s 1s to overlap with $\mathbf{x}$'s 1s.

*when $k$ and $l$ are well-defined (as in Definition 3), otherwise the probability is* $0$.

**Proof 3** *We prove Eq. (3.13), and let the reader verify Eq. (3.14). We fix* $\mathbf{x}$*, and think of* $\mathbf{y}$ *as the binary string that we vary so that we may look at the event* $E' = \{\mathbf{y} | \textit{exactly } m \textit{ of } \mathbf{y}\textit{'s } l \ 1s \textit{ overlap with } \mathbf{x}\textit{'s } k \ 1s\}$. *We can count the number of* $\mathbf{y}$ *that satisfies* $E'$ *by choosing* $m$ $1s$ *in* $\mathbf{y}$ *from positions out of the* $k$ $1$*-positions in* $\mathbf{x}$*, which is* $\binom{k}{m}$*, and then choosing the remainder* $l-m$ $1s$ *in* $\mathbf{y}$ *from positions out of the* $n-k$ $0$*-positions in* $\mathbf{x}$*, which is* $\binom{n-k}{l-m}$*. The multiplication counting rule gives* $|E'| = \binom{k}{m}\binom{n-k}{l-m}$*. Now if we vary* $\mathbf{x}$*, by the multiplication rule we have* $|E| = \binom{n}{k}\binom{k}{m}\binom{n-k}{l-m}$*. There are a total of* $\binom{n}{k}\binom{n}{l}$ *pairs of* $(\mathbf{x}, \mathbf{y})$ *of specified weights. Since all such pairs have the same probability, we can take the ratio of* $|E|$ *over the total number of pairs, giving us Eq. (3.13).*

**Theorem 1** *Let* $E$ *be the event that the number of* $1s$ *in* $\mathbf{X}$ *and* $\mathbf{Y}$ *overlap in exactly* *m positions. Define:*

$$a(k,m) = \begin{cases} \binom{k}{m} & \textit{if } k \geq m \\ 0 & o.w \end{cases} \tag{3.15}$$

$$b(k,l,m) = \begin{cases} \binom{n-k}{l-m} & \textit{if } n-k \geq l-m \\ 0 & o.w \end{cases} \tag{3.16}$$

$$c(k) = \begin{cases} \binom{n}{k} & \textit{if } n \geq k \\ 0 & o.w \end{cases} \tag{3.17}$$

*In addition, we define $\binom{a}{b}$ to be equal to 0 if either $a$ or $b$ are not integers. Then:*

$$Pr(E) = \sum_{k=1}^{n}\sum_{l=1}^{n} a(k,m)b(k,l,m)c(k)p^k(1-p)^{n-k}q^l(1-q)^{n-l} \tag{3.18}$$

**Proof 4**

$$\begin{aligned} & Pr(\{w(\mathbf{X}) = k \textit{ and } w(\mathbf{Y}) = l \textit{ and}\} \cap E) \\ = \; & Pr(E|\{w(\mathbf{X}) = k \textit{ and } w(\mathbf{Y}) = l\}) \\ & \cdot Pr\{w(\mathbf{X}) = k\}Pr\{w(\mathbf{Y}) = l\} \qquad (3.19) \\ = \; & \frac{\binom{k}{m}\binom{n-k}{l-m}}{\binom{n}{l}}\binom{n}{k}p^k(1-p)^{n-k}\binom{n}{l}q^l(1-q)^{n-l} \qquad (3.20) \end{aligned}$$

*Eq. (3.20) follows from Lemma 3, where again we assume $k$ and $l$ are well-defined, or the probability is 0. Finally we can extract the desired marginal distribution:*

$$Pr(E) = \sum_{k=1}^{n}\sum_{l=1}^{n} Pr(\{w(\mathbf{X}) = k \textit{ and } w(\mathbf{Y}) = l \textit{ and}\} \cap E) \tag{3.21}$$

**Corollary 1**

$$\begin{aligned} & Pr\{w(\mathbf{X}) = w(\mathbf{X} \oplus \mathbf{Y})\} \\ = \; & \sum_{k=1}^{n} \sum_{l \textit{ is even}}^{n} a\left(k, \frac{l}{2}\right) b\left(k, l, \frac{l}{2}\right) c(k) \\ & \qquad \cdot p^k(1-p)^{n-k}q^l(1-q)^{n-l} \qquad (3.22) \end{aligned}$$

*where $a(k,m)$, $b(k,l,m)$, $c(k)$ are as defined in Theorem 1.*

**Proof 5** *Apply Lemma 1 to Theorem 1.*

We are ready to state our first result as the solution to Problem 1.

**Solution 1** *The stealth condition $\mathcal{S} = Pr\{w(\mathbf{X}) = w(\mathbf{X} \oplus \mathbf{Y})\}$ is given by*

$$\begin{aligned}\mathcal{S} &= \sum_{k=1}^{n} \sum_{l \text{ is even}}^{n} a\left(k, \frac{l}{2}\right) b\left(k, l, \frac{l}{2}\right) c(k) \\ &\qquad \cdot p^k (1-p)^{n-k} q^l (1-q)^{n-l} \end{aligned} \tag{3.23}$$

*where $a(k,m)$, $b(k,l,m)$, $c(k)$ are as defined by*

$$a(k,m) = \begin{cases} \binom{k}{m} & \text{if } k \geq m \\ 0 & o.w \end{cases} \tag{3.24}$$

$$b(k,l,m) = \begin{cases} \binom{n-k}{l-m} & \text{if } n-k \geq l-m \\ 0 & o.w \end{cases} \tag{3.25}$$

$$c(k) = \begin{cases} \binom{n}{k} & \text{if } n \geq k \\ 0 & o.w \end{cases} \tag{3.26}$$

Before investigating the implications of solution 1, we proceed to the relaxed version of the stealth condition via the study of Problem 2.

**Corollary 2** *Let $\epsilon$ be a positive integer. Then:*

$$\begin{aligned} & Pr\{|w(\mathbf{X}) - w(\mathbf{X} \oplus \mathbf{Y})| < \epsilon\} \\ &= \sum_{m=\lceil \frac{l-\epsilon}{2} \rceil}^{\lfloor \frac{l+\epsilon}{2} \rfloor} \sum_{k=1}^{n} \sum_{l=1}^{n} a(k,m)\, b(k,l,m)\, c(k) \\ &\qquad \cdot p^k (1-p)^{n-k} q^l (1-q)^{n-l} \end{aligned} \tag{3.27}$$

*where $a(k,m)$, $b(k,l,m)$, $c(k)$ are as defined in Theorem 1.*

**Proof 6** *Given realizations* $\mathbf{x}$ *and* $\mathbf{y}$*, let* $k = w(\mathbf{x})$ *and* $l = w(\mathbf{y})$*.*

$$|w(\mathbf{x}) - w(\mathbf{x} \oplus \mathbf{y})| < \epsilon \tag{3.28}$$

$$\Rightarrow \begin{cases} k < k + l - 2m + \epsilon \\ k > k + l - 2m - \epsilon \end{cases} \tag{3.29}$$

*The second line relies on the proof for Lemma 1. Since the events of strings having* $1$*s overlapping in exactly* $m'$ *and* $m''$ *positions are disjoint, the probability of the union of the events is the sum of the probabilities of the individual events.*

The solution to Problem 2 readily follows from Corollary 2.

**Solution 2** *The relaxed form of the stealth condition* $\mathcal{S}'$ *for the direct stealthy attack game is given by:*

$$\begin{aligned} \mathcal{S}' &= Pr\{|w(\mathbf{X}) - w(\mathbf{X} \oplus \mathbf{Y})| < \epsilon\} \\ &= \sum_{m=\lceil \frac{l-\epsilon}{2} \rceil}^{\lfloor \frac{l+\epsilon}{2} \rfloor} \sum_{k=1}^{n} \sum_{l=1}^{n} a\,(k,m)\, b\,(k,l,m)\, c(k) \\ &\qquad \cdot p^k (1-p)^{n-k} q^l (1-q)^{n-l} \end{aligned} \tag{3.30}$$

*where* $\epsilon$ *is an integer and* $a(k,m)$*,* $b(k,l,m)$*,* $c(k)$ *are as defined in Theorem 1.*

We are now in a position to address Problem 3 where the goal is the determination of the best probability $q$ that a hostile sensor network should employ given that the probability $p$ (based on local sensor threshold $T_h$) is not known. We answer this question for sufficiently large sensor densities in Theorem 2.

**Theorem 2** *For* $n$ *sufficiently large,* $q^* \downarrow 0$ *as* $n \to \infty$*, where* $q^* = \arg\max_{q \in [0,1]} \mathcal{S}$*, that is,* $q^* = \arg\max_{q \in [0,1]} Pr\{w(\mathbf{X}) = w(\mathbf{X} \oplus \mathbf{Y})\}$*.*

**Proof 7** *Let $\varphi(q) = Pr\{w(\mathbf{X}) = w(\mathbf{X} \oplus \mathbf{Y})\}$ where $p$ is treated as a fixed constant.*[2] *As $n \to \infty$, $w(\mathbf{X})/n \overset{a.s.}{\to} p$ and similarly $w(\mathbf{Y})/n \overset{a.s.}{\to} q$. Using this idea (which could also be strengthened using strong typicality), it can be shown that $w(\mathbf{x}) \approx np$ and $w(\mathbf{y}) \approx nq$ for all realizations $\mathbf{x}$ and $\mathbf{y}$ for sufficiently large $n$. Hence substituting $k = np$ and $l = nq$ into Eq. (3.23), we obtain:*

$$\varphi(q) \approx \binom{np}{nq/2}\binom{n(1-p)}{nq/2}\binom{n}{np}p^{np}(1-p)^{n(1-p)}q^{nq}(1-q)^{n(1-q)} \tag{3.31}$$

*when $n$ is sufficiently large. The conditions for being well-defined imply $q \leq \min\{2p, 2(1-p)\}$, which can readily be verified. Again for sufficiently large $n$, we apply Stirling's approximation ($n! \approx (n/e)^n$) to Eq. (3.31).*

$$\varphi(q) \propto \frac{(1-q)^{n(1-q)}}{\left(\frac{n}{2}\right)^{nq}[n(p-q/2)]^{n(p-q/2)}[n(1-p-q/2)]^{n(1-p-q/2)}} \tag{3.32}$$

*In Eq. (3.32), we have removed the non-negative constants (independent of $q$). Next we examine the derivative of $\varphi(q)$.*

$$\begin{aligned}\frac{\partial\varphi(q)}{\partial q} \quad \propto \quad & 2^{nq-1}n^{1-nq}(1-q)^{n(1-q)} \\ & \cdot[n(1-p-q/2)]^{-n(1-p-q/2)}[n(p-q/2)]^{-n(p-q/2)} \\ & \cdot \ln\left(\frac{4(p-q/2)(1-p-q/2)}{(1-q)^2}\right)\end{aligned} \tag{3.33}$$

*We can verify that the point $q = 0$ is a salient point (i.e. a "corner" since $\varphi(q)$ "turns on" at $q = 0$) so the derivative does not exist at this point. Hence our discussion of the derivative is restricted to $0 < q \leq \min\{2p, 2(1-p)\}$. Under the implications for being well-defined, it can be verified that the terms outside* ln *are always non-negative*

[2] *The difficulty in this proof lies not in taking the derivative of $\varphi(q)$, but rather in solving the first order condition $\partial\varphi(q)/\partial q = 0$; hence we resort to the asymptotic case as well as approximations. We also note that although $q^*$* approaches 0, *setting $q^* = 0$ is incorrect, as this results in $\varphi(0) = 0$.*

*(Appendix A). However, the* $\ln$ *term can be shown to be non-positive by showing that the argument inside* $\ln$ *is always* $\leq 1$ *(Appendix A). Therefore* $\partial\varphi(q)/\partial q \leq 0$ *over the interval of* $q \in (0, \min\{2p, 2(1-p)\}]$ *implies* $\varphi(q)$ *is monotonically decreasing in this interval. The maximum* $q^*$ *must then be the left boundary, i.e* $q^* \downarrow 0$*.*

Theorem 2 suggests that when $n$ is large, the hostile sensor network should be looking for an optimal $q$ that is quite small. This result is important since $\varphi(q)$ is not concave and hence utilization of numerical methods to find the optimal $q$ benefits from a good initialization.

**Solution 3** *In a stealthy direct attack, each hostile node* $h_i$ *should attack with* $q^* = \zeta$ *where* $\zeta$ *is closer to* $0$ *than to* $0.5$ *when* $n$ *is sufficiently large. This ensures the maximization of the stealth condition* $\mathcal{S}$ *and hence of the probability that the attack is undetected for this choice of* $q^*$*.*

Theorem 2 also provides general information regarding the power of the attack $P_a$ under the strict stealth $\mathcal{S}$ condition as specified in Corollary 3.

**Corollary 3** *Suppose that the hostile sensor network plays* $q^*$ *according to Theorem 2. Let* $l = E[w(\mathbf{Y})]$ *be the average expected number of legitimate bits that are flipped. Then* $l \ll n$*.*

**Proof 8** *Since* $l = nq^*$*, therefore* $l/n = (nq^*)/n = q^* \ll 1$*, which implies* $E[w(\mathbf{Y})] \ll n$*.*

For the static stealthy direct attack game $\mathcal{G}$, the pure strategy Nash equilibria are the strategy vectors $(p^*, q^*)$ ($p^* \in [0,1]$, $q^* \in [0,1]$) such that Player 1 would not find it beneficial to deviate from $p^*$ given Player 2 plays $q^*$, and vice versa. This problem is generally difficult, but if we look at the asymptotic case again, that is for $n$ sufficiently large, it can be shown that $p^*$ and $q^*$ are again close to some boundary.

**Theorem 3** *Suppose that Player* 1 *can select* $p^*$ *from a closed subinterval* $[0, 1]$ *denoted* $P = [a, b]$*,* $a < b$*, while* $q^* \in [0, 1]$*. For* $n$ *sufficiently large, the pure strategy Nash equilibrium is given by:*

$$p^* = \begin{cases} a & \textit{if } a < |1-b| \\ b & \textit{if } a > |1-b| \end{cases} \tag{3.34}$$

*and* $q^* = \zeta$*, where* $\zeta \downarrow 0$*. If* $a = |1 - b|$*, then there are two equilibria at* $(a, \zeta)$ *and* $(b, \zeta)$*.*

**Remark 1** *The expression in Eq. (3.34) refers to choosing the left-most boundary if it is closer to* 0 *than the right-most boundary is closer to* 1*, and choosing the right-most boundary if it is closer to* 1 *than the left-most boundary is closer to* 0*.*

**Proof 9** *First we find the best response of Player* 2 *to Player* 1*'s* $p$*. We have already shown in Theorem 2 that* $q^* \downarrow 0$ *as* $n \to \infty$*. For* $q^*$ *sufficiently small, we can assume it is irrespective of* $p$*. Next we examine the best response of Player* 1 *to Player* 2*'s* $q$*, where we know that* $q$ *will always be approaching* 0*. With this in mind, we define* $\phi(p)$ *for* $q$ *fixed at* $q^*$*:*

$$\phi(p) = \sum_{k=1}^{n} \sum_{l \textit{ is even}}^{n} \binom{l}{l/2} \binom{n-l}{k-l/2} \binom{n}{l} q^l (1-q)^{n-l} p^k (1-p)^{n-k} \tag{3.35}$$

*where we have used Eq. (3.14) instead of Eq. (3.13). Now since* $q^*$ *is small,* $nq^* \ll n$ *so* $\binom{n}{l} q^l (1-q)^{n-l}$ *can be approximated by a Poisson distribution* $\lambda^l / l! e^{-\lambda}$*, where* $\lambda = nq^*$*.*

$$\begin{aligned} \phi(p) &\approx \sum_{k=1}^{n} \sum_{l \textit{ is even}}^{n} \binom{l}{\frac{l}{2}} \binom{n-l}{k-\frac{l}{2}} \frac{\lambda^l}{l!} e^{-\lambda} p^k (1-p)^{n-k} && (3.36) \\ &\approx \sum_{k=1}^{n-1} \binom{2}{1} \binom{n-2}{k-1} \frac{\lambda^2}{2!} e^{-\lambda} p^k (1-p)^{n-k} && (3.37) \end{aligned}$$

*where we have kept only the smallest* $l = 2$ *in the series, as* $\lambda^l$ *for* $l \geq 4$ *is insignificant*

*[94]. Next we use the identity:*

$$\binom{n-2}{k-1} + \binom{n-2}{k} = \binom{n-1}{k} \tag{3.38}$$

$$\begin{aligned}
\phi(p) &\approx \lambda^2 e^{-\lambda}\Bigg\{ \sum_{k=1}^{n-1} \binom{n-1}{k} p^k (1-p)^{n-k-1}(1-p) \\
&- \sum_{k=1}^{n-2} \binom{n-2}{k} p^k (1-p)^{n-k-2}(1-p)^2 \Bigg\} \qquad (3.39) \\
&= \lambda^2 e^{-\lambda}\Bigg\{ (1-p)\left[\sum_{k=0}^{n-1} \binom{n-1}{k} p^k (1-p)^{(n-1)-k}\right] - (1-p)^n \\
&- (1-p)^2 \left[\sum_{k=0}^{n-2} \binom{n-2}{k} p^k (1-p)^{(n-2)-k}\right] + (1-p)^n \Bigg\} \qquad (3.40)
\end{aligned}$$

*where in the last line we have extended $k$ to start at $0$ in the series, and hence must subtract/add the $k = 0$ term to maintain equality. We have chosen to do this because each of the series sum to $1$ as both series represent the total sum of a binomial distribution. The expression then simplifies to:*

$$\begin{aligned}
\phi(p) &\approx \lambda^2 e^{-\lambda}\left\{(1-p) - (1-p)^2\right\} \qquad (3.41) \\
&= \lambda^2 e^{-\lambda}(p - p^2) \qquad (3.42)
\end{aligned}$$

*This shows that $\phi(p)$ is approximated as a concave function with peak at $p = 1/2$ when $n$ is sufficiently large. If $p$ can be chosen from the entire interval $[0, 1]$, then the minima of $\phi(p)$ would be at $p^* = 0$ and $p^* = 1$. If instead we have to choose $p$ from the closed subinterval $P \subset [0, 1]$, then we would take either the left or right boundary, whichever is closer to $0$ or $1$ respectively.*

The result of Theorem 3 is an approximation for sufficiently large $n$, so it does not predict games involving average-sized sensor networks. Again we only have some guidelines as to where to search for the pure strategy Nash equilibrium or equilibria.

If the left and right boundary of $P$ are equally close to 0 and 1 respectively, then there are two equilibria. This suggests a symmetry in $p$, which is stated in Theorem 4

**Theorem 4** *Define $\psi(p,q) = Pr\{w(\mathbf{X}) = w(\mathbf{X} \oplus \mathbf{Y})\}$, where both $p$ and $q$ are now variable. Let $\bar{p} = 1 - p$, then $\psi(p,q) = \psi(\bar{p},q)$.*

**Proof 10** *Write:*

$$\begin{aligned}
& \psi(\bar{p},q) \\
= \; & \sum_{k=1}^{n} \sum_{l \text{ is even}}^{n} \binom{k}{l/2}\binom{n-k}{l/2}\binom{n}{k}\bar{p}^k(1-\bar{p})^{n-k}Q(l) && (3.43) \\
= \; & \sum_{x=1}^{n} \sum_{l \text{ is even}}^{n} \binom{n-x}{l/2}\binom{x}{l/2}\binom{n}{n-x} \\
& \qquad \cdot (1-p)^{n-x}p^xQ(l) && (3.44) \\
= \; & \sum_{x=1}^{n} \sum_{l \text{ is even}}^{n} \binom{n-x}{l/2}\binom{x}{l/2}\binom{n}{x}(1-p)^{n-x}p^xQ(l) && (3.45) \\
= \; & \psi(p,q) && (3.46)
\end{aligned}$$

*where $Q(l) = q^l(1-q)^{n-l}$. In Eq. (3.45) we used the substitution $x = n - k$, and in Eq. (3.45) we used the identity $\binom{a}{b} = \binom{a}{a-b}$. One can also easily verify that the conditions for being well-defined hold by substituting $k = n - x$.*

**Solution 4** *Two competing sensor networks $L$ and $H$ should play relatively small $p$ (or large $\bar{p}$) and relatively small $q$ in the static game when $n$ is sufficiently large in order to minimize and maximize the stealth condition $\mathcal{S}$ respectively.*

In the next section we discuss the results derived above for the hostile network H as well as their implications for sensor networks of varying cluster size $n$.

## 2. Attack Performance

In the above section we derived theoretical predictions of how two competing sensor networks affect each other. The results were mainly of existence and asymptotic

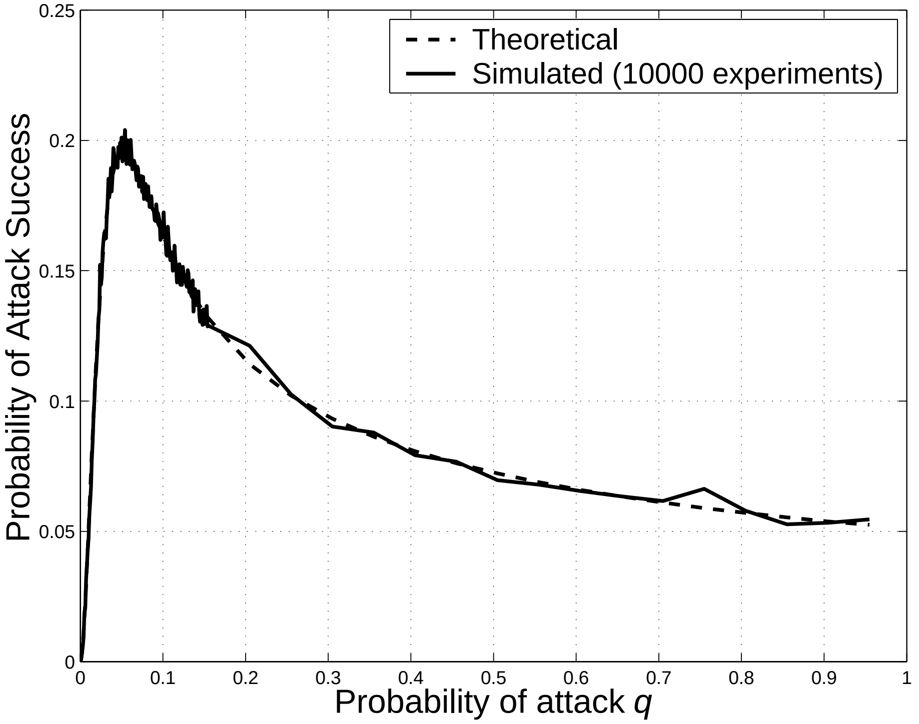


Fig. 15. Theoretical vs. simulated $\varphi(q)$, probability of stealthy attack success, for $n = 60$ nodes, $p = 0.495$ (probability bit 1 is sent by legitimate node).

nature. In this section we examine realistic finite sized networks and discuss some trends not explicitly stated by the theorems to assess the performance of the attack under the stealth condition in the case of direct stealthy attacks.

We first examine a plot of $\varphi(q)$ which corresponds to the probability of attack success or more precisely to the stealth condition $\mathcal{S}$ for a given value of probability $p$. As seen in Figure 15, the theoretical curve from Eq. (3.23) and the simulated curve based on $10^5$ experiments match closely. Furthermore for sensor networks of size $n = 60$ and $p = 0.495$, it is seen that the optimal attack probability $q$ is $q^* \approx 0.05$, which is closer to 0 than to 0.5 and thus in agreement with both Solutions 3 and 4. Importantly we note that the probability of attack success $\varphi(q)$ (i.e. the stealth

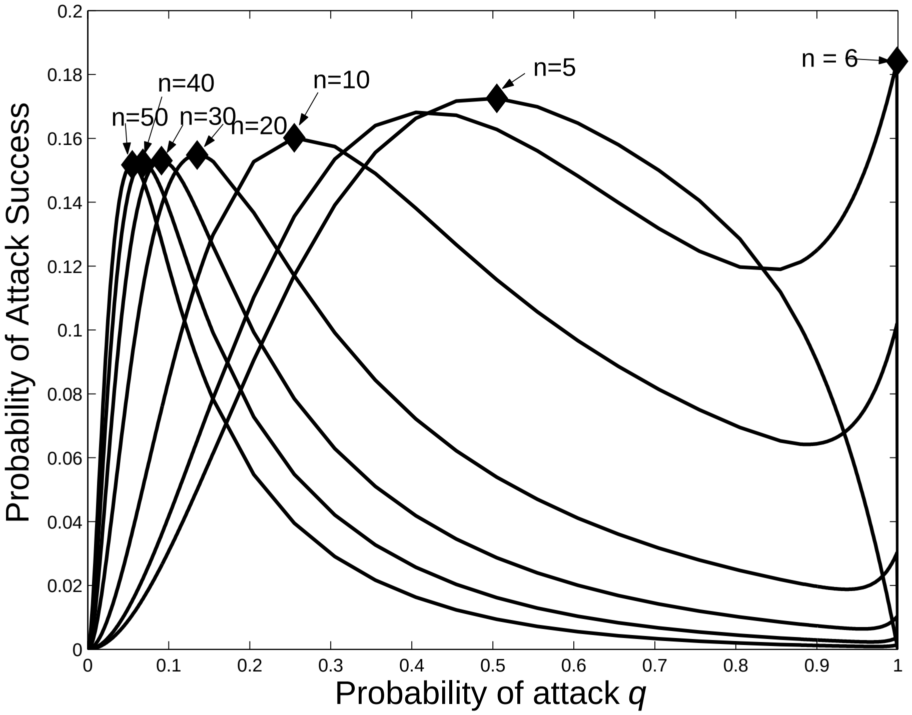


Fig. 16. Probability of stealthy attack success, $\varphi(q)$, for $p = 0.3$ (probability bit 1 is sent by legitimate node) over various network sizes $n$.

condition) is a *relative* measure of stealth as described in Chapter II. Thus a higher value of $\varphi(q)$ is advantageous for the hostile network while a lower value of $\varphi(q)$ is advantageous for the legitimate network. As will be shown in Section D, this relative measure corresponds to the probability of attack detection such that higher values of $\varphi(q)$ (corresponding to greater stealth) correspond to a lower probability of the attack being detected. As such, the stealth metric is consistent for both H and L.

The dynamics of the optimal $q^*$ which vary with varying $n$ can be seen in Figure 16. We note that as $n$ becomes larger, the peak $q^*$ approaches 0 as indicated by Solution 3. Most importantly, this is not generally the case for arbitrarily small $n$. Indeed for certain values of $n$ based on the underlying combinatorics, the peak may

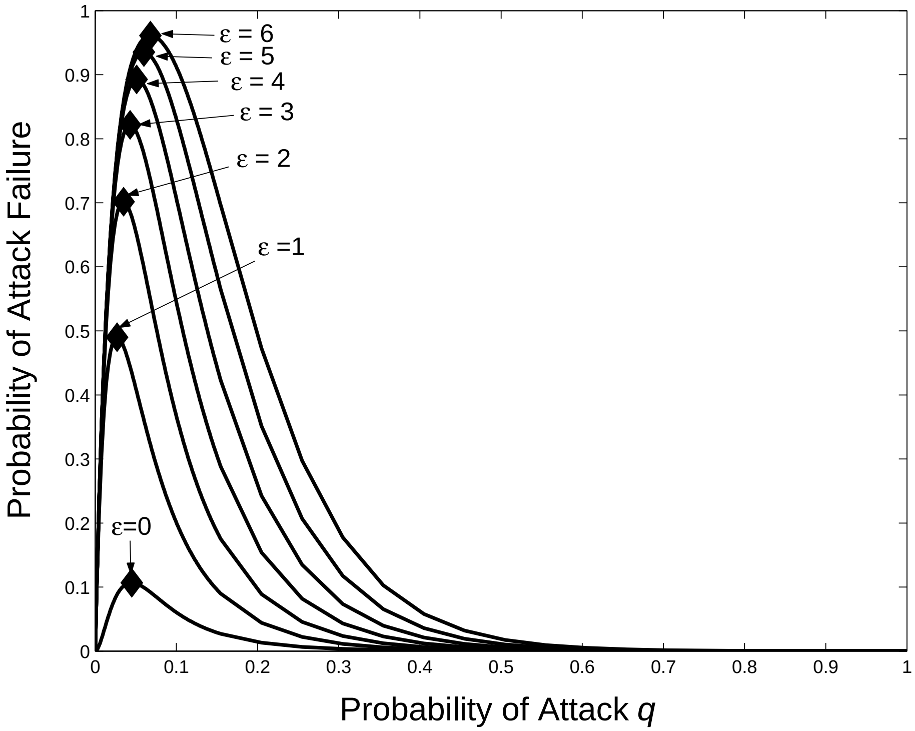


Fig. 17. Probability of stealthy attack failure, $1 - \varphi(q)$, for $n = 55$ nodes, $p = 0.2$ (probability bit 1 is sent by legitimate node) over various $\epsilon$ uncertainty.

arise closer to $q = 1$. This indicates that the hostile network should attack with high probability while obtaining a comparably high level of (relative) stealth. This does not contradict the theoretical predictions of Solution 3 since the latter were obtained for sufficiently large $n$. Intuitively this can also be understood from the fact that $\varphi(q)$ is a positive weighted sum of semi-concave functions in $q$ (i.e. $q^l(1-q)^{n-l}$) where such a sum need not be semi-concave [95] as is demonstrated in Figure 16. The observations regarding the cluster size $n$ have implications for the defense strategies of the legitimate network $L$ which we will discuss.

In solution 2 the stealth condition $\mathcal{S}$ was relaxed by a factor of $\epsilon$ to produce a new modified stealth condition $\mathcal{S}'$ which is given by Eq. (3.30). Figure 17 shows the effect of varying $\epsilon$ on the relative probability that the attack will be *detected*, that is, the vertical axis depicts the probability of anti-stealth $1 - \varphi(q)$ for a given value of $p$. We note that as $\epsilon$ is increased, the peak of the anti-stealth (i.e. relative detection) curve increases, thus *decreasing* H's stealth and increasing the chance of attack detection. Importantly, relaxing the stealth condition by even the small factor of $\epsilon = 1$ (shown in Figure 17 for the case of $n = 55$ and $p = 0.2$) increases the relative probability of attack detection significantly. For the case shown in Figure 17, the probability of attack failure (i.e. the attack is detected) increases from approximately 0.1 to 0.5. This result is very intuitive in that relaxing the average statistical similarity of the $\mathbf{x}$ and $\mathbf{z}$ vectors by even a small factor can cause the count at the cluster head to depart from the count expected by the cluster head under the case of no attack. Thus we conclude that the stealth condition is a very strict condition as previously stipulated. Satisfying this strict condition is important for the hostile network given a lack of knowledge regarding the specific attack detection mechanisms utilized by the legitimate network.

Next we examine the overall game $\mathcal{G}$ via the $\psi(p, q)$ manifold for the two sensor networks of size $n = 60$ as shown in Figure 18. The legitimate network L (Player 1) wishes to minimize the probability of attack success (i.e. the stealth condition $\mathcal{S}$) while the hostile network (Player 2) wishes to maximize it. If Player 1 can choose from the entire interval then Player 1 will choose $p = 0$ or $p = 1$ on the $p$-axis of Figure 18 as predicted by Theorem 3. Player 2 chooses a probability $q$ that maximizes Figure 18. As can be seen from Figure 18, any choice of $q$ given Player 1's choice of $p = 0, 1$ will result in an attack success probability of 0. This result agrees with the expectation that if the cluster head always expects $\mathbf{z} = \mathbf{0}$ (the all-zero vector) or $\mathbf{z} = \mathbf{1}$ (the all-one vector), then no attack can misguide the cluster head. In the proof of Theorem 3 we showed that the peak on the $p$-$\psi$ plane is always at $p = 0.5$ and in

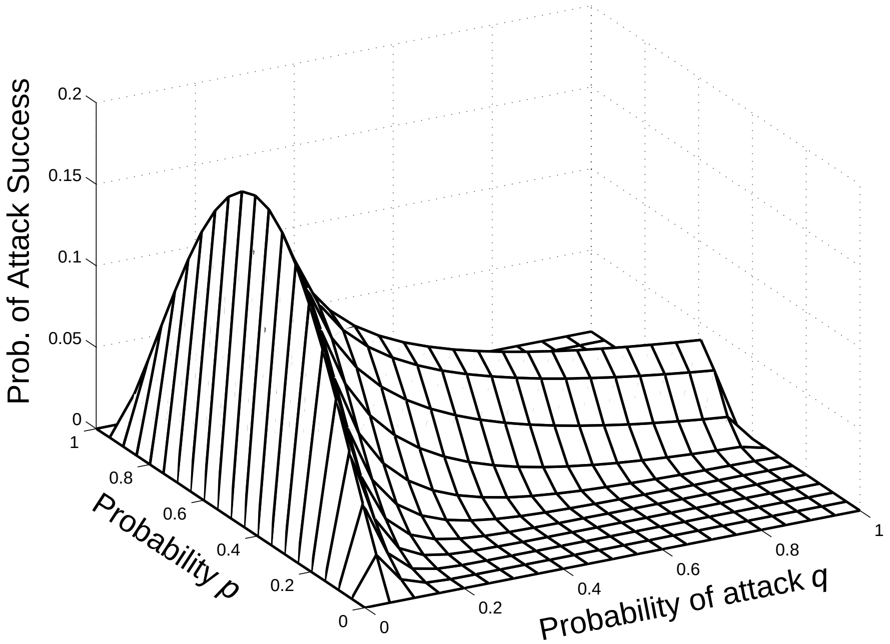


Fig. 18. Probability of stealthy attack success, $\psi(p,q)$, for $n = 60$ nodes.

Theorem 4 we showed that this trace is symmetrical in $p$. These features are readily verified in Figure 18 and carry implications for the defense strategies of L in terms of local threshold $T_h$ selection which yields the probability $p$ of witnessing an event.

### 3. Attack Implications

Having examined the salient features of the game for both networks, we now expand upon the significance of these results for both attack and defense strategies. The stealth condition of Eq. (3.23) (or more generally (3.30)) is unfortunately cumbersome to inspect. Plotting Eq. (3.23) for different values of cluster size $n$ and probability of an event $p$ nevertheless yields a unique value of probability $q$ that maximizes the stealth condition (i.e. it is the global peak of Eq. (3.23)). The results of such plotting

Table I. Optimal $q^*$ Value for Cluster Size $n$ and Probability of Event $p$

| $n$ | $p = 0.01$ | $p = 0.05$ | $p = 0.1$ | $p = 0.2$ | $p = 0.3$ | $p = 0.4$ | $p = 0.5$ |
|---|---|---|---|---|---|---|---|
| 2 | 0.9990 | 0.9990 | 0.9990 | 0.9990 | 0.9990 | 0.9990 | 0.9990 |
| 5 | 0.4050 | 0.4050 | 0.4050 | 0.4550 | 0.5050 | 0.5050 | 0.5050 |
| 10 | 0.2050 | 0.2050 | 0.2050 | 0.2550 | 0.2550 | 0.9990 | 0.9990 |
| 20 | 0.1010 | 0.1050 | 0.1100 | 0.1220 | 0.1350 | 0.1470 | 0.1520 |
| 30 | 0.0670 | 0.0700 | 0.0740 | 0.0820 | 0.0910 | 0.0990 | 0.1030 |
| 40 | 0.0500 | 0.0530 | 0.0550 | 0.0620 | 0.0680 | 0.0750 | 0.0780 |
| 50 | 0.0400 | 0.0420 | 0.0440 | 0.0490 | 0.0550 | 0.0600 | 0.0620 |
| 100 | 0.0200 | 0.0210 | 0.0220 | 0.0250 | 0.0280 | 0.0300 | 0.0310 |

are summarized in Table I which shows the optimal value of attack probability $q^*$ for each pair $(n, p)$ (the stealth condition is symmetric in $p$ and thus the effect of $p$ is the same as the effect of $1 - p$ and we only consider $p \in [0, 0.5]$). We make a few key observations regarding this result. For a *given* value of cluster size $n$ (i.e. a row in Table I), $q^*$ is almost constant to within one significant digit irrespective of the value of probability $p$. Thus if the attacker knows the cluster size $n$, he can determine the optimal value of attack without having to know the probability $p$. This is significant since the value of $p$ depends in part on a sensor's threshold selection $T_h$ and may not always be available to the attacker [6].

Examination of Table I also yields important insights regarding the dynamic relationship between the cluster size $n$ and the optimal attack parameter $q^*$. We observe that as $n$ increases, $q^*$ decreases for all values of $p$. This result can be understood in the context of typical sets if we consider the $n$ sensor decisions as a string of length $n$. The typical set is usually a small set but with probability of occurrence close to 1. When $n$ is small, the typical set is small but relatively large compared to the set of all possible strings of length $n$. When $n$ increases, the set of all possible strings of length $n$ grows to be very large and the size of the typical set is *relatively* much smaller. Thus it becomes more difficult for the attacker to attack the "string" and still remain in the typical set. This implies that the chance of attack on the sensors decreases but this decrease may also carry ramifications for the *detection* of such an attack as we will explore in Section D.

The results of Table I also support the analytical results from solution 4 for the legitimate network. Such analysis reveals that the optimal value of $p$ for $p \in [0, 0.5]$ is $p^*$ *small* (the optimal value of $p$ for $p \in [0.5, 1]$ is $p^*$ *large*). This suggests that to improve the attack detection, the sensors should be calibrated to have a small (or large) value of $p$ through threshold $T_h$ selection if such selection is possible (depending on the underlying technology of the sensor). Indeed if we examine more of the significant digits in the results of Table I, the optimal value of $q^*$ does indeed decrease with decreasing $p$ with ramifications for attack detection which is examined in Section D. The implications of these results for the hostile network in terms of carrying out a stealthy direct attack are summarized in Algorithm 1.

### D. Secure Data Acquisition Results

In this section we investigate attack detection and mitigation strategies at the cluster head in the case of direct stealthy attacks. As modeled in Section B, the cluster head receives decisions regarding an event from $n$ sensors that may be attacked by hostile nodes deployed in the area. Importantly we show how game theoretic analysis of the optimal attack strategies from Section D-C enables the use of established detection techniques to uncover the attack and mitigate its effects.

**Algorithm 1** Stealthy Direct Attack Algorithm for Hostile Network

```
Ensure: Min attack detection and power of defense given legitimate network whose
    detection paradigm and defense mechanisms are not known.
 1: if legitimate cluster size $n$ is not known: then
 2:     Select a large cluster size where large signifies $n \geq 30$
 3: end if
 4: if $p$ is not known then
 5:     Select a small value of $p$ where small signifies $p \leq 0.1$
 6: end if
 7: Find the value of $q^*$ based on $(n, p)$ and Eq. (3.23).
 8: if both $(n, p)$ are known then
 9:     The value of $q^*$ is optimal and exact.
10: else if only $n$ is known then
11:     The value of $q^*$ is approximate to within one significant digit.
12: else
13:     The value of $q^*$ is a worst case scenario approximation.
14: end if
15: Find the relative stealth $\mathcal{S}$ based on $q^*$ and Eq. (3.23).
16: Find the expected power of the attack $E[P_a] = nq^*$.
17: if the relative stealth $\mathcal{S}$ is desirable then
18:     The optimal $q^*$ has been found.
19: else
20:     Decrease the value of $q^*$. Return to step 15.
21: end if
```

### 1. Defense Analysis

In detection problems we are generally faced with the task of deciding between two or more hypotheses based on received data. The Neyman-Pearson (NP) detector is an optimal detector appropriate for cases where a priori probabilities of the hypotheses are not available, and for cases where the probability of detection $P_D$ and the probability of false alarm $P_{FA}$ may not be of equal significance to the application (otherwise a Bayesian detector may be appropriate). According to the NP approach, we obtain a detector by maximizing $P_D$ for a desired false alarm rate $P_{FA} = \alpha$. The resulting optimal detector is a *likelihood ratio* detector $\Lambda(\mathbf{z})$ given by Eq. (3.47), where $\mathbf{z}$ is the received data vector, where the comparison threshold $\mathcal{T}$ is chosen according to Eq. (3.48) and where randomization may need to be performed if $\Lambda(\mathbf{z}) = \mathcal{T}$ to achieve the desired $\alpha$.

$$\Lambda(\mathbf{z}) = \frac{p(\mathbf{z};\mathcal{H}_1)}{p(\mathbf{z};\mathcal{H}_0)} \underset{H_0}{\overset{H_1}{\gtrless}} \mathcal{T} \tag{3.47}$$

$$P_{FA} = \sum_{\mathbf{z}:\Lambda(\mathbf{z})>\mathcal{T}} p(\mathbf{z};\mathcal{H}_0)\ d\ \mathbf{z} \leq \alpha \tag{3.48}$$

For the case of $n$ binary sensors, the data vector $\mathbf{z}$ consists of Bernoulli random variables from a distribution which is $Bern(p)$ (hypothesis $\mathcal{H}_0$) or a distribution $Bern(r)$ (hypothesis $\mathcal{H}_1$) as given by Eq. (3.49). By applying Eq. (3.47) it can easily be shown that the NP detector for this case is given by Eq. (3.50), where $w(\mathbf{z})$ is the weight (the number of 1s) in the data vector $\mathbf{z}$.

$$\begin{aligned} \mathcal{H}_0 &: \text{ normal operation}, \mathbf{Z} \sim Bern(p) \\ \mathcal{H}_1 &: \text{ attacked operation}, \mathbf{Z} \sim Bern(r) \end{aligned} \tag{3.49}$$

$$\Lambda(\mathbf{z}) = \frac{r^{w(\mathbf{z})}(1-r)^{n-w(\mathbf{z})}}{p^{w(\mathbf{z})}(1-p)^{n-w(\mathbf{z})}} \underset{H_0}{\overset{H_1}{\gtrless}} \mathcal{T} \tag{3.50}$$

$$\sum_{\mathbf{z}:\Lambda(\mathbf{z})>\mathcal{T}} p^{w(\mathbf{z})}(1-p)^{n-w(\mathbf{z})} \leq \alpha \tag{3.51}$$

The threshold $\mathcal{T}$ is chosen to satisfy a desired $\alpha$ based on Eq. (3.51), where the summation is over all the possible data vectors $\mathbf{z}$ such that $\Lambda(\mathbf{z})$ exceeds $\mathcal{T}$. However this is equivalent to summing over all possible weights $w$ for $w \in [0, n]$ as shown in Eq. (3.52). The notation $\mathbf{I}_P$ denotes the indicator function which is equal to 1 if $P$ is true and is equal to 0 otherwise. Finally, the probability of detection $\beta$ resulting from the use of the $\Lambda(\mathbf{z})$ detector is given by Eq. (3.53).

$$\sum_{w=0}^{n} \tbinom{n}{w} p^{w(\mathbf{z})} (1-p)^{n-w(\mathbf{z})} \ \mathbf{I}_{\ \Lambda(\mathbf{z})>\mathcal{T}} \ \leq \alpha \tag{3.52}$$

$$\beta = \sum_{w=0}^{n} \tbinom{n}{w} r^{w(\mathbf{z})} (1-r)^{n-w(\mathbf{z})} \ \mathbf{I}_{\ \Lambda(\mathbf{z})>\mathcal{T}} \tag{3.53}$$

To distinguish between normal operation and an attack/fault, the cluster head must therefore employ the detection statistic (likelihood ratio $\Lambda$) of Eq. (3.50) and compare it to the threshold $\mathcal{T}$ that is set based on Eq. (3.52) with the resulting probability of detection given by Eq. (3.53). Importantly, the detection statistic $\Lambda(p, r)$ depends on the value of $p$ and $r$. Hence in the case of an attack with unpredictable probability, the detection statistic depends on the *unknown* underlying parameter $q$ since $r = p + q - 2pq$. The detection statistic's dependence on $q$ also translates into difficulties in determining the probability of false alarm and detection based on the dependence of Eqs. (3.52) and (3.53) on $\Lambda$.

Thus although we have determined an optimal attack detector for the cluster head, it is not implementable in its current form unless the parameter $q$ is known. Fortunately we can re-arrange the likelihood ratio $\Lambda$ as shown in Eq. (3.54) where $(1-r)^n/(1-p)^n$ is equal to a positive constant $k > 0$ for all values of $0 \leq r \leq 1$, $0 \leq p < 1$ and $n$. Let us for the moment assume that $r > p$ in Eq. (3.54). Then it can easily be seen that $\Lambda(w) = k(r/p)^w((1-p)/(1-r))^w$ is monotonically increasing in $w$ where we have written $\Lambda$ in terms of $w$ to simplify the notation and emphasize the role of the "aggregate" statistic (the weight $w$) in lieu of the original data vector $\mathbf{z}$.

$$\Lambda(z) = \frac{r^{w(\mathbf{z})}(1-r)^{n-w(\mathbf{z})}}{p^{w(\mathbf{z})}(1-p)^{n-w(\mathbf{z})}} = \frac{(\frac{r}{1-r})^{w(\mathbf{z})}}{(\frac{p}{1-p})^{w(\mathbf{z})}} \frac{(1-r)^n}{(1-p)^n} = k\left(\frac{r}{p}\right)^{w(\mathbf{z})}\left(\frac{1-p}{1-r}\right)^{w(\mathbf{z})} \tag{3.54}$$

Based on the monotonicity of $\Lambda$, we may now invoke the Karlin-Rubin theorem [96] to obtain an alternative form for the cluster head detector with the same $P_D$-$P_{FA}$ performance. The alternative form for the cluster head detector is given by Eqs. (3.55), (3.56) and (3.57) where $p'$ is a probability of mixing between the two hypotheses if $w$ is precisely equal to $\mathcal{T}$ (the mixing probability $p'$ is set based on Eq. (3.56) for a desired $\alpha$). As shown in Eq. (3.58), based on the assumption that $r > p$, these equations are valid for the interval where $p < 1/2$. When $p \in [1/2, 1]$, the hypotheses in Eq. (3.55) are switched.

$$w \underset{H_0}{\overset{H_1}{\gtrless}} \mathcal{T} \tag{3.55}$$

$$if \quad w = \mathcal{T} \quad then \quad declare \quad H_1 \quad w.p \quad p'$$

$$\alpha = \sum_{w>\mathcal{T}}^{n} \tbinom{n}{w}(\frac{p}{1-p})^w(1-p)^n + p'\tbinom{n}{\mathcal{T}}(\frac{p}{1-p})^{\mathcal{T}}(1-p)^n \tag{3.56}$$

$$\beta = \sum_{w>\mathcal{T}}^{n} \tbinom{n}{w}(\frac{r}{1-r})^w(1-r)^n + p'\tbinom{n}{\mathcal{T}}(\frac{r}{1-r})^{\mathcal{T}}(1-r)^n \tag{3.57}$$

$$r > p \Rightarrow \quad p + q - 2pq > p \quad \Rightarrow \quad p < \frac{1}{2} \tag{3.58}$$

We observe that the detection statistic $w$ and the comparison threshold $\mathcal{T}$ in Eq. (3.55) no longer require the cluster head to know the value of $q$ and thus the detector is implementable at the cluster head. We note however that in order to determine the resulting probability of detection $P_D$, the value of $r$ (and thus $q$) is still required in Eq. (3.57). Thus for the case of an attack, analysis of the optimal attack $q$ as addressed in Section C is required in order to determine the detector's performance.

We also note that the detection statistic is now a simple weight and thus the cluster head must merely count the number of 1's that it has received from the $n$ sensors and compare this count to a threshold. The optimal NP detector at the cluster head is thus identical in form to the detectors often used in practical implementations as discussed in Section B (in such implementations the comparison threshold may be set based on experimental trials or based on an expected average count of $c \pm \epsilon^3$) [7], [3], [16]. The optimal NP detector however makes use of a threshold $\mathcal{T}$ that is set based on a desired probability of false alarm $\alpha$ and based on the probability $p$ of an event. Setting the threshold based on Eq. (3.56) thus provides a greater level of control and flexibility to meet the $P_{FA}$ requirements of the application. Furthermore, this detector is guaranteed to provide the best probability of detection $P_D$ for a chosen $P_{FA} = \alpha$ (a property of Neyman-Pearson detectors). In Section 2 we examine the actual performance of this cluster head detector and compare it to the performance of a detector based on the expected average $c \pm \epsilon$.

## 2. Defense Performance

Based on the model of Section B, a detector for attack identification at the cluster head may be based on the Neyman-Pearson design or on an average expected count $c$ where $c \approx np \pm \epsilon$ for a cluster size of $n$ sensors with probability of event $p$. In this section we wish to compare the performance of these two approaches and also obtain some general insights into the $P_D$-$P_{FA}$ performance curve for different values of $p$ and $n$ and for various attack probabilities $q$.

[3] This $\epsilon$ should not be confused with the $\epsilon$ relaxation factor in the modified stealth condition $\mathcal{S}'$.

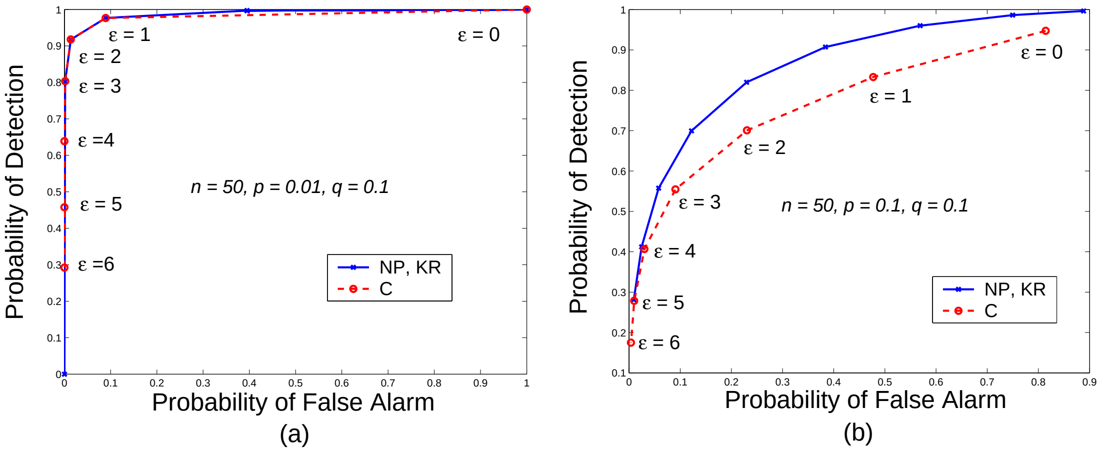


Fig. 19. (a) $n = 50$, $p = 0.01$ and $q = 0.1$. (b) $n = 50$, $p = 0.1$ and $q = 0.1$.

In Figures 19a and 19b, as well as in Figure 20, the $P_D$-$P_{FA}$ performance of the NP and $c \pm \epsilon$ detectors are depicted for $n = 50$ sensors, various $(p, q)$ pairs and various values of $\epsilon$ "slack" in the $c$ detector. As can be seen from these figures, the performance of the average expected $c$ detector follows the general trend of the NP detector although it typically does not achieve the same overall performance. Nevertheless, by choosing a different value of $\epsilon$, it is possible to achieve a desired trade-off between the probability of detection $P_D$ (vertical axis) and the probability of false alarm $P_{FA}$ (horizontal axis). The average expected $c$ detector may thus be useful for certain applications, in particular ones where the probability of an event $p$ is expected to be small (based on the phenomenon of interest and the selection of the sensor threshold $T_h$) as in Figure 19a. As a side note, we observe that the performance of the NP detector based on Eqs. (3.50), (3.52) and (3.53) which we denote by "NP" is the same as the performance of the NP detector based on the Karlin-Rubin simplification of Eqs. (3.55), (3.56) and (3.57) which we denote by "KR" in Figures 19a and 19b and in Figure 20. Thus we are justified in utilizing the simplified form of the NP detector to obtain the same performance.

Importantly based on Figures 19 and 20, we observe that the NP detector per-

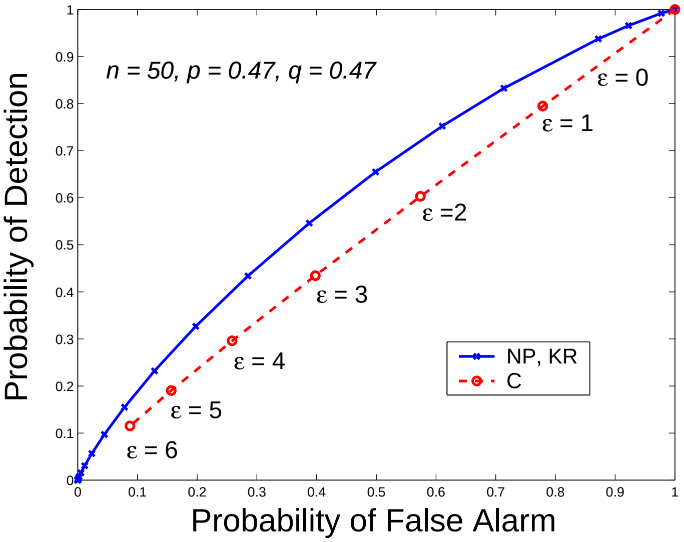
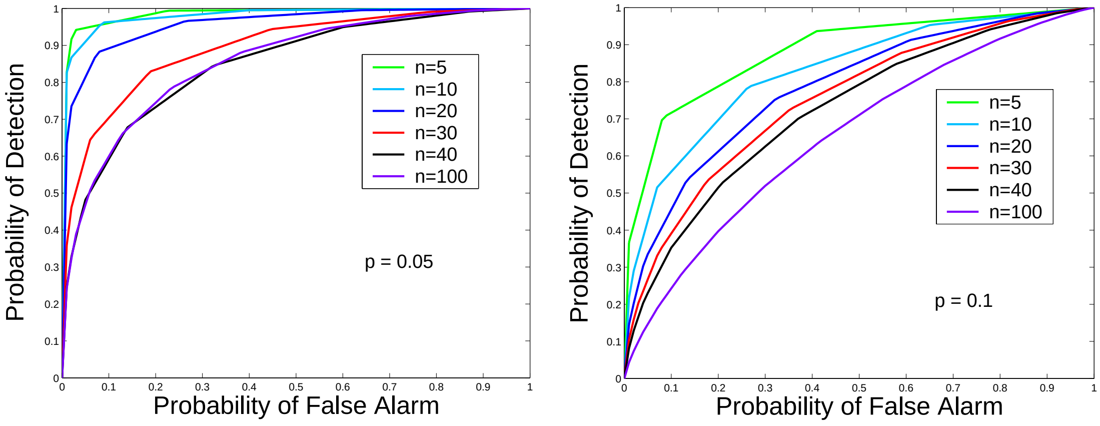


Fig. 20. $n = 50$, $p = 0.47$ and $q = 0.47$.

forms better for smaller values of probability $p$ for $p \in [0, 0.5]$. By symmetry for $p \in [0.5, 1]$, it performs better for values of $p$ closer to 1. This result is consistent with the results of Section C where based on analysis of the stealth condition of Eq. (3.23) we noted that it was best to calibrate the sensors to a small value of $p$ or to a large value of $p$. Indeed based on Figures 19 and 20 and the results of Table I, the worst $P_D$-$P_{FA}$ performance is obtained for values of $p$ closest to $p = 0.5$. This can be understood from Eq. (3.58) where $r = p + q - 2pq$. When $p = 0.5$, $r = 0.5$ and thus the detector is not able to distinguish between the $H_0$ and $H_1$ hypotheses. At an intuitive level, when $p = 0.5$, the probability of obtaining a decision bit of value 1 is the same as the probability of obtaining a sensor decision bit of value 0. This situation corresponds to the largest level of uncertainty that the cluster head can experience and makes it easier for an attacker to fool the detector.

Based on these results we are able to confirm the previous assertion regarding the consistency of the stealth condition for the legitimate and hostile networks.



(a) (b)

Fig. 21. The $P_D$-$P_{FA}$ performance curves for various values of $n$ and the optimal value of $q^*$ corresponding to that $n$ for (a) $p = 0.05$ and (b) $p = 0.1$.

**Remark 2** *The stealth condition $\mathcal{S}$ of Eq. (3.23) is a relative measure of the hostile network's stealth and is a consistent measure for both the legitimate and hostile networks in terms of the probability of detecting the attack such as under the Neyman-Pearson paradigm.*

### 3. Defense Implications

In the previous section we compared the performance of the NP and $c$ detectors for various values of the probability $p$ with implications for the selection of a local sensor threshold $T_h$. We now wish to explicitly investigate the performance of the NP detector for an *optimal* attack parameter $q^*$ as obtained from Section C. Figure 21a depicts the $P_D$-$P_{FA}$ performance of the NP detector for $p = 0.05$ and for various values of cluster size $n \in [5, 100]$. Crucially, each performance curve is obtained assuming the value of attack parameter $q$ that is *optimal* for the given $(n, p)$ pair as obtained in Table I or directly from the stealth condition $\mathcal{S}$ in Eq. (3.23). Figure 21b is obtained similarly but for a value of $p = 0.1$.

Based on these two figures, we make the important observation that the $P_D$-

$P_{FA}$ performance *decreases* as the number of sensors $n$ is *increased.* This somewhat surprising result is an outcome of the stealth condition of the attacker. That is, *if* the attacker is *not* stealthy, increasing the number of sensors will increase the detection performance. If however the attacker is *stealthy*, then he selects an optimal value of $q^*$ based on Eq. (3.23) or Table I. As discussed in Section C, this optimal value of $q$ decreases with increasing cluster size $n$. Thus the attack becomes more rare in the sense that the average expected power of the attack $E[P_a] = nq_{|q=q^*}$ decreases, which is a desirable property. At the same time however, it becomes more difficult to detect the attack when it does occur. The implications of these results for attack detection and mitigation for the legitimate sensor network are summarized via Algorithm 2.

Finally we make a brief but important observation regarding the sensor decision threshold $T_h$ and the role that cryptography plays in the competing networks scenario. As noted in Chapter II Section D-1, encryption mechanisms do not protect the data against a hostile attack that occurs during the collection process. In this sense, *forward* data encryption, that is encryption between the sensors and the sink, does not protect against the actuation attacks (though this forward encryption is required to protect the data during its dissemination). Interestingly we note that for the competing networks scenario, it is the *backward* encryption of data between the sink and the sensors that plays an important role. As discussed in Section C and summarized in Algorithm 1, the hostile network benefits from knowledge of the sensor threshold $T_h$. Consequently the legitimate network benefits from keeping the value of $T_h$ secret in addition to setting its value to a desirable level. If the hostile network estimates (or otherwise obtains) the value of $T_h$, the sink of the legitimate network benefits from re-issuing a new value of $T_h$ to its sensors. It may also instruct the sensors to set their thresholds to obtain a probability of event $p = 0$ or $p = 1$ in order to “catch” the hostile network in the midst of attack. Such re-issuing through the backward channel must be encrypted in order to be effective.

**Algorithm 2** Defense Algorithm for Legitimate Network

```
Ensure: Max attack detection and power of defense given competing hostile network.
1: Given the probability density function (pdf) of the phenomenon, set the local sensor threshold $T_h$:
2: if events are expected to be common then
3:     Set $T_h$ such that $p$ (area under the pdf to the left of $T_h$) is close to 1.
4: else
5:     Set $T_h$ such that $p$ is close to 0.
6: end if
7: Select a value of cluster size $n$.
8: Find attacker's $q^*$ based on $(n, p)$ pair and Eq. (3.23).
9: Find the defense's $P_D$-$P_{FA}$ based on $q^*$ from Eqs. (3.55), (3.56) and (3.57).
10: Find the defense's expected power of defense $E[P_d] = 1 - nq^*$.
11: if $P_D$-$P_{FA}$ and $E[P_d]$ are appropriate for the application then
12:     cluster size $n$ and decision threshold $T_h$ have been determined.
13: else
14:     Return to step 7 and select a higher value of $n$.
15: end if
```

## E. Stealthy Direct Attack Comparisons

In the previous sections we have derived the stealth condition $\mathcal{S}$ for the case of a direct stealthy attack. We determined that this condition is consistent for both the legitimate and hostile networks such that it can be utilized to obtain the optimal defense and attack strategies. In this section we wish to compare the stealthy direct

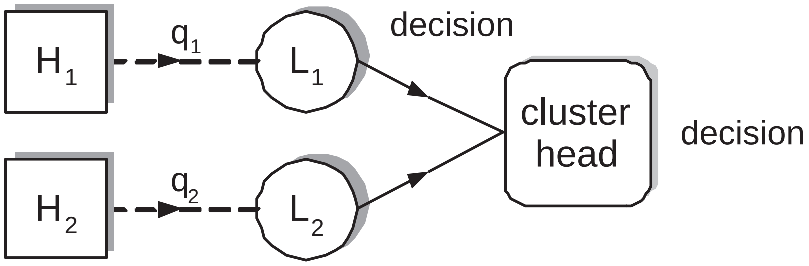


Fig. 22. Two hostile nodes deployed against two legitimate nodes. Each hostile node may actuate with a different probability $q_i$.

attack to a stealthy attack where the hostile nodes must actively communicate with each other. We also compare the direct stealthy attack to the case of an uncoordinated stealthy attack where each hostile node may select a different attack strategy. We show interesting properties of these attacks and demonstrate that the direct stealthy attack achieves a favorable stealth $\mathcal{S}$ performance and a good power-communication-detection $PCD$ performance compared with the other two stealthy attacks. These results carry important implications for the design of attack and defense strategies.

### 1. Comparison with Uncoordinated Attack

In the direct stealthy attack, each hostile node optimizes its attack parameter based on the knowledge that every other hostile node is utilizing the same attack parameter. That is, $q_i = q \ \forall \ i \in \{1, \ldots, n\}$ which enables each hostile node to solve for $q^*$ in the stealth condition $\mathcal{S}$ of Eq. (3.23). To assess the direct stealthy attack, we compare it with the uncoordinated stealthy attack [97]. In the uncoordinated attack, each hostile node may utilize a *different* attack parameter $q_i$ as shown in Figure 22.

Specifically we consider the scenario where $n = 2$ hostile nodes are actuating against two legitimate sensors as shown in Figure 22. We employ the same data acquisition and attack models as in Section B. That is, we assume that the case where a legitimate sensor $i$ witnesses an event of interest when the attack is absent is denoted by $x_i = 1$, and that this event occurs with Bernoulli probability $p$ such that $Pr(X_i = 1) = p$. Conversely $x_i = 0$ denotes the condition where no event of interest is recorded by sensor node $i$ when actuation is absent and this event carries probability $Pr(X_i = 0) = 1-p$. The action of a hostile node $i$ is denoted by $Y_i$ where the realization $y_i = 1$ denotes attack and $y_i = 0$ denotes no attack. We assume that the Bernoulli probability that a hostile node $y_i$ actuates is given by $Pr(Y_i = 1) = q_i$. Let $\mathbf{x} = [x_1 x_2]$, $\mathbf{y} = [y_1 y_2]$ and $\mathbf{z} = [z_1 z_2]$. We examine the case where the stealth relaxation parameter is $\epsilon = 0$ and thus in order to evade detection, each node $i$ in the hostile network wishes to maximize it's utility function $\pi_i$ given by Eq. (3.59) which depends on the parameter $q_i$ that it chooses, as well as on the parameter $q_j$ that the other hostile node chooses independently. Importantly $\pi_i$ from Eq. (3.59) still depends on the probability of an event $p$ as was the case in the direct stealthy attack, though this is not emphasized in Eq. (3.59) where $q_i$ is the focus.

$$\pi_i(q_1, q_2) = Pr\{w(\mathbf{X}) = w(\mathbf{Z})\} = Pr\{w(\mathbf{X}) = w(\mathbf{X} \oplus \mathbf{Y})\} \tag{3.59}$$

The probability of Eq. (3.59) can be expressed and simplified as shown in Eqs. (3.60) to (3.63). The final simplified utility function $\pi_i(q_1, q_2)$ is given by Eq. (3.64) which has been written to emphasize the form of the interaction between $q_1$ and $q_2$.

$$\begin{aligned} Pr\{w(\mathbf{X}) = w(\mathbf{Z})\} = {} & Pr\{w(\mathbf{X}) = w(\mathbf{Z}) | \mathbf{X} = 00\} \cdot Pr\{\mathbf{X} = 00\} \\ & + Pr\{w(\mathbf{X}) = w(\mathbf{Z}) | \mathbf{X} = 01\} \cdot Pr\{\mathbf{X} = 01\} \\ & + Pr\{w(\mathbf{X}) = w(\mathbf{Z}) | \mathbf{X} = 10\} \cdot Pr\{\mathbf{X} = 10\} \\ & + Pr\{w(\mathbf{X}) = w(\mathbf{Z}) | \mathbf{X} = 11\} \cdot Pr\{\mathbf{X} = 11\} \end{aligned} \tag{3.60}$$

$$\begin{aligned} Pr\{w(\mathbf{X}) = w(\mathbf{Z})\} = Pr\{(w(Y_1) = 0 \wedge w(Y_2) = 0)\} \cdot (1-p)^2 + \\ Pr\{(w(Y_1) = 0 \wedge w(Y_2) = 0) \vee (w(Y_1) = 1 \wedge w(Y_2) = 1)\} \cdot 2p(1-p) + \\ Pr\{(w(Y_1) = 0 \wedge w(Y_2) = 0)\}p^2 \end{aligned} \quad (3.61)$$

$$\begin{aligned} Pr\{w(\mathbf{X}) = w(\mathbf{Z})\} = Pr\{[w(Y_1) = 0 \wedge w(Y_2) = 0]\} \cdot (1-p)^2 + \\ 2 \cdot [Pr\{(w(Y_1) = 0 \wedge w(Y_2) = 0) \vee (w(Y_1) = 1 \wedge w(Y_2) = 1)\} \cdot p(1-p)] + \\ Pr\{[w(Y_1) = 0 \wedge w(Y_2) = 0]\} \cdot p^2 \end{aligned} \quad (3.62)$$

$$\begin{aligned} Pr\{w(\mathbf{X}) = w(\mathbf{Z})\} = (1-q_1)(1-q_2)(1-p)^2 + \\ ((1-q_1)(1-q_2) + q_1 q_2) \cdot 2p(1-p) + (1-q_1)(1-q_2) \cdot p^2 \end{aligned} \quad (3.63)$$

$$\begin{aligned} \Pi_i(q_1, q_2) &= \alpha \cdot (q_1 + q_2) + \beta_p \cdot (q_1 \cdot q_2) + \gamma \quad i = \{1, 2\} \\ \alpha &= -1 \\ \beta_p &= -2p^2 + 2p + 1 \\ \gamma &= 1 \end{aligned} \quad (3.64)$$

Based on the utility of Eq. (3.64), it can be shown (Appendix A) that the best response $B_i(q_j)$ of node $i$ to a strategy $q_j$ of node $j$ is given by Eq. (3.65), where $T_p$ is a threshold point that depends on $\beta_p$ from Eq. (3.64) (and hence on parameter $p$, that is, the probability of an event under no attack). The intersection(s) of the best response functions of the players (if any) provide the set of Nash equilibria of the game. It can be shown based on Eqs. (3.64) and (3.65) that there are two pure action Nash equilibria $(q_{1,N}, q_{2,N})$ for this game as given by Eq. (3.66), and that the resulting utility $\pi_i(q_{1,N}, q_{2,N})$ for node $i$ at each equilibrium is given by Eq. (3.67).

$$\begin{aligned} B_i(q_j) = 0 \quad if \quad q_j < T_p \\ B_i(q_j) = 1 \quad if \quad q_j > T_p \\ T_p = \frac{1}{\beta_p} \\ \beta_p \in [1, 1.5] \end{aligned} \tag{3.65}$$

$$(q_{1,N}, q_{2,N}) = \{(0,0), (1,1)\} \tag{3.66}$$

$$\pi_i(0,0) = 1 \qquad \pi_i(1,1) = \beta_p - 1 \tag{3.67}$$

To better illustrate the interaction of the hostile nodes and the consequences of the game, Figure 23 depicts the stealth $\mathcal{S}$ utility manifold $\pi_i(q_1, q_2)$ between the two hostile nodes over the entire domain of $q_1$ and $q_2$. The two Nash equilibria occur at $(q_{1,N}, q_{2,N}) = (0, 0)$ and $(q_{1,N}, q_{2,N}) = (1, 1)$ as predicted via Eq. (3.66) and as confirmed by examining the best response intersections shown in Figure 24. We note two salient features of this result which we will examine further:

**1.** In contrast with the direct stealthy attack, when each hostile node $i$ is permitted to choose its *own* attack parameter $q_i$ more than one pure Nash equilibrium emerges. Specifically, for the $n = 2$ case in the direct stealthy attack, the unique optimal value of $q$ is $q^* = 0.999 \approx 1$ (for all values of $p$). However for the $n = 2$ and independent $q_i$'s case, two extreme optimal values of $q_i$ emerge. One such value occurs at $q_i = 0$ and the other at $q_i = 1$, thus directing each hostile node to attack either with probability 0 or with probability 1.

**2.** The threshold or dividing point $T_p$ between the two equilibria depends solely on the parameter $\beta_p$ and thus on the underlying probability of an event $p$ which is

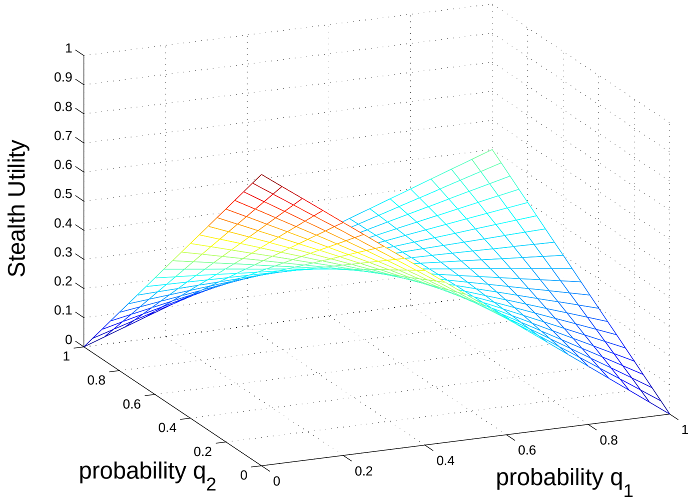


Fig. 23. Stealth utility manifold for a hostile node $i$ versus the full set of actions $q_1$ and $q_2$ for the case where $p = 0.5$. The two Nash equilibria for this game occur at $(0, 0)$ and $(1, 1)$ and the $T_p$ threshold is the saddle point.

*not* controlled by the hostile nodes and may not be known due to its dependence on the legitimate node's threshold $T_h$.

We now expand upon the significance of these two points. The emergence of a second equilibrium and the dependence of a hostile node's decision threshold $T_p$ on $p$ raises two new questions. Namely we are presented with the question of *how* a hostile node will select its action and with the question of *which* equilibrium will actually occur. If the two hostile nodes have a means of direct communication, it suffices for the two nodes to agree upon a common action where both nodes pick $q = 0$ or both nodes pick $q = 1$. This type of attack with dynamic communication is examined in the next section.[4] Importantly, agreement between the two nodes may be reached

[4] We note that communication among the hostile nodes must also remain "stealthy" (in a sense relevant to the given application) for the attack to go unnoticed overall.

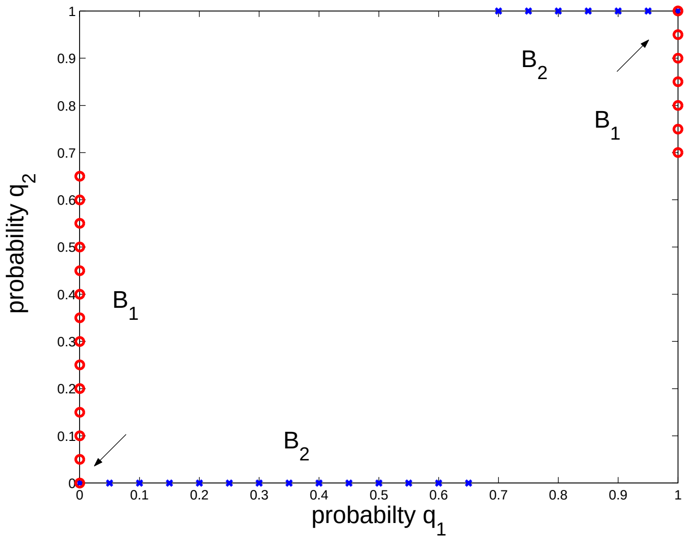
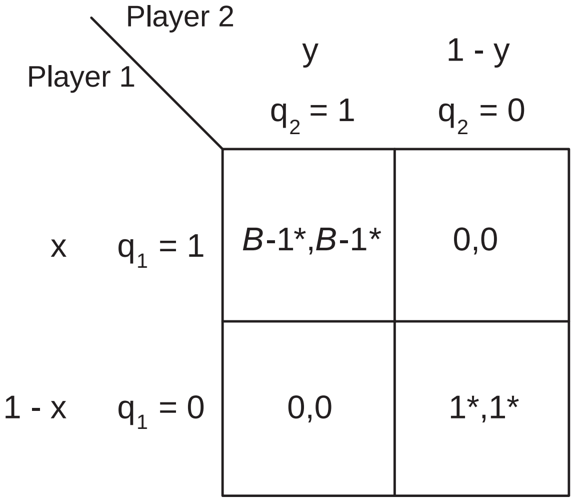


Fig. 24. Best response functions of hostile nodes $h_1$ and $h_2$ showing the two Nash equilibria at the intersection points.

instead by means of strategy mixing. To describe the process of strategy mixing, we assume for the moment that both hostile nodes can determine the probability density function of the phenomenon (such as through observations over time) and with an approximation of the threshold $T_h$ can thus obtain the approximate value of the probability $p$. Despite this information, each hostile node still needs to know if the other hostile node will choose a value of probability $q$ below or above $T_p$ to choose its best $q$ (Eq. (3.65)) given no communication.

In the absence of such knowledge, each hostile node may *mix* between its pure optimal actions of $q = 0$ and $q = 1$ with some probability as shown in Figure 25. We assume that Player 1 (hostile node 1) chooses action $q_1 = 0$ with some probability $x$ and that it chooses $q_1 = 1$ with probability $1 - x$. Similarly, Player 2 (hostile node 2) chooses action $q_2 = 0$ with probability $y$ and $q_2 = 1$ with probability $1 - y$. The new utility $\pi_i(x, y)$ obtained by node $i$ based on its mixing variable $x$ and the mixing



| Player 1 \ Player 2 | | y<br>$q_2 = 1$ | 1 - y<br>$q_2 = 0$ |
|---|---|---|---|
| x | $q_1 = 1$ | *B*-1*,*B*-1* | 0,0 |
| 1 - x | $q_1 = 0$ | 0,0 | 1*,1* |

Fig. 25. A mixed-action game with mixing probabilities $x$ and $y$. The $(u_1, u_2)$ numbers inside each cell represent the utility of player 1 and 2 respectively.

variable of the other node $y$ is given by Eq. (3.68). It can thus be shown that a third *mixed* strategy Nash equilibrium emerges, where the optimal Nash $x$ and $y$ mixes are given by Eq. (3.69) along with the corresponding utility $\pi_i(x_N, y_N)$ at equilibrium given by Eq. (3.70).

$$\pi_i(x, y) = xy + (1 - x)(1 - y)(\beta_p - 1) \tag{3.68}$$

$$(x_N, y_N) = (\frac{1}{\beta_p}, \frac{1}{\beta_p}) \tag{3.69}$$

$$\pi_i(x_N, y_N) = \frac{1}{\beta_p} \tag{3.70}$$

We make three key observations regarding this result. First we observe that the mixing probabilities only depend on $\beta_p$ (and thus on the probability $p$) and do not require the nodes to know each other's actions. The second observation regarding the new *mixed* equilibrium reveals an interpretation for the $T_p$ threshold dividing the two pure action equilibria. We examine Eq. (3.64) and suppose that hostile node 1 plays with $q_1$ set to $T_p$, that is, $q_1 = 1/\beta_p$. We observe that the resulting utility $\pi_2$ for hostile node 2 is given by $\pi_2(q_1 = T_p, q_2) = 1 - 1/\beta_p$. Thus the utility of node 2 is independent of its own $q_2$ selection or in other words, node 2 is *indifferent* in its $q_2$. Furthermore, the achieved utility of $1 - 1/\beta_p$ is *equal to* the utility achieved at mixed equilibrium shown in Eq. (3.70). By the properties of mixed equilibria [56], these two observations imply that the $T_p$ threshold (saddle point in Figure 23) *is* the mixed strategy equilibrium. Finally the third observation is that the range and maximum value of the new utility $\pi_i(x_N, y_N) \in [0, 0.5]$ is generally smaller than the range and maximum of the previous utility $\pi_i(q_{1,N}, q_{2,N}) \in [0, 1]$. Eliminating direct communication and eliminating implicit coordination (implemented via the $q_i = q$ $\forall i$ condition) thus comes at the price of a decrease in the utility (i.e. stealth of the attack) and can be understood as the associated cost.

Based on these three observations we obtain the following comparison between the uncoordinated attack and the direct stealthy attack. The stealth $\mathcal{S}$ *benefit* of coordination via the $q_i = q$ $\forall i$ condition is captured analytically through Eq. (3.70) and can be seen directly in Figure 23 for the case of $n = 2$ hostile nodes. In Figure 23, the $(q_1, q_2) = (1, 1)$ point results in the maximal (relative stealth measure) $\mathcal{S}$ and corresponds to the coordinated attack. In the same figure, the saddle point $(q_1, q_2) = (1/\beta_p, 1/\beta_p)$ yields the lowest $\mathcal{S}$ and corresponds to the case of no coordination. Intuitively this loss in stealth performance stems from the uncertainty that arises due to the existence of two possible pure Nash equilibria. For the hostile network, this result captures the tradeoff between coordination via the $q_i = q \forall i$ condition and between the achieved stealth $\mathcal{S}$. For the legitimate network, this result signifies that hostile nodes do not need to communicate directly with each other to carry out a stealthy attack (where communication may presumably reveal the attack). In the next section we explicitly examine the case of active hostile node communication.

### 2. Comparison with Active Communication Attack

We consider the situation where hostile nodes are able to communicate with each other directly prior to an attack to select the optimal attack strategy to achieve a power of attack while maintaining stealth. For this comparison we employ the power-communication-detection $PCD$ metric given in Eq. (3.71) which takes into account the number of communications required for the attack. In the context of a stealthy attack, the significance of communication is that each use of it among the hostile nodes may potentially reveal the attack to the legitimate network and thus requires special methodologies (such as the use of spread spectrum covert communications).

$$PCD = \frac{\text{No. attacked nodes}}{(1 + \text{No. communications}) \cdot (1 + P_D)} \tag{3.71}$$

As in the case of the uncoordinated attack, for the comparison we assume that the hostile nodes are able to estimate the probability density function of the phenomenon and the local decision threshold $T_h$ of the legitimate nodes. Based on such knowledge and based on its own local readings of the source $O$, each hostile node is able to decide if its neighboring legitimate node will produce a decision bit of value 1 or 0 as given in Eq. (3.1). Thus as a group, the hostile network is able to determine the weight $w$ that the legitimate nodes wish to report to the cluster head prior to the attack. We denote this pristine weight prior to the attack by $w_x$ (in relation to the notation $\mathbf{x}$ which denotes the pristine sensor decisions).

Importantly based on such group knowledge, H is able to achieve the maximal power of attack $P_a$ which is still stealthy (where $P_a$ is the number of sensor decisions that are altered). That is, each sensor decision may be flipped from 1 to 0 or vice versa provided that the overall weight $w_x$ is maintained. As an example, if there are ten sensors and three of them would report a 1 (i.e. $n = 10$ and $w_x = 3$), then the hostile network can flip all three 1s to a value of 0 and find three 0s to flip to a 1. Thus $P_a = 3$. If $n = 10$ and $w_x = 7$, the hostile network can still only flip three 1s to a 0 and find three 0s to flip to a 1. The hostile network cannot flip all seven 1's to 0's because of the "lack of zeros" to flip back to ones. The power of the attack in the second example is thus still $P_a = 3$. More generally, subject to the stealth constraint $\mathcal{S}$, H achieves the maximal power of attack $P_a$ in the active communications case which is given by Eq. (3.72).

$$P_a = \min(w_x, n - w_x) \tag{3.72}$$

This result however can only be achieved if the hostile nodes are able to communicate actively with each other, that is, they are able to exchange information on the actual conditions that each hostile node encounters prior to the attack. We consider a simplified communication algorithm to achieve this goal with the aim of obtaining the minimum number of communications that are required for this process. The minimum is used mainly for simplicity of analysis and represents the best case scenario for the active communications attack. In this communication algorithm, each hostile node that has a bit of value 1 broadcasts its desire to do a "flip" process. Each hostile node with a value of 0 responds to one such broadcasting hostile node. If collisions occur, any efficient resolution process may be utilized. For instance, a broadcasting node accepts the first received bid, confirms it and ends the broadcast. An example of such a communication process is summarized in Algorithm 3 for each hostile node.

To estimate the minimum number of required communications however, we assume that no collisions occur. Based on the assumption of no collisions, no acknowl-

**Algorithm 3** Example of a Communication Algorithm for each Hostile Node

```
Ensure: Power of the attack $P_a$ must satisfy $P_a = \min(w_x, n - w_x)$
 1: Determine if the legitimate sensor will report a bit of value 1 or 0.
 2: if legitimate sensor will report a bit of value 1 then
 3:     Broadcast to other hostile nodes that you have a 1, until bids are received.
 4:     Accept a bid (such as the first bid) and end the broadcast.
 5: else
 6:     Listen for broadcasts and issue bid (such as to closest broadcasting node).
 7:     if confirmation from broadcasting node is received: then
 8:         Accept the match-up.
 9:     else
10:         Return to step 6.
11:     end if
12: end if
```

edgements of the receipt of a bid are required. The communications are thus due to the original broadcast calls from each node that has a bit 1. Thus the minimum number of required communications under this paradigm is easily determined to be $\min(w_x, n - w_x)$. Thus the PCD metric for the active communications attack which we denote by $PCD_c$ is given by Eq. (3.73). The corresponding PCD metric for the direct stealthy attack which we denote by $PCD_d$ is given by Eq. (3.74). As can be seen, the direct stealthy attack does not incur any communication costs (it relies on coordination instead). However it generally does not achieve the same maximal power of attack $P_a$ as the active communications attack. Indeed each hostile node attacks with an optimal probability $q^*$ and the overall number of altered sensor decisions is $\min(w_y, n - w_y)$ which may approximately equal $\min(nq^*, n - nq^*)$ on average for $n$ hostile nodes.

$$PCD_c = \frac{\min(w_x, n - w_x)}{(1 + \min(w_x, n - w_x)) \cdot (1 + P_D)} \tag{3.73}$$

$$PCD_d = \frac{\min(w_y, n - w_y)}{1 \cdot (1 + P_D)} \tag{3.74}$$

The average power of the attack $P_a$ for the active communications attack and the direct stealthy attack are compared for various cluster sizes $n$ and different probabilities $p$ in Figure 26. We make some important observations regarding this result. First we recall that the active communications attack achieves the maximal $P_a$ that maintains perfect stealth $\mathcal{S}$. The direct stealthy attack relies only on stealth coordination and does not always satisfy $\mathcal{S}$ perfectly. Interestingly, the latter coordination tactic actually translates into a higher power of attack $P_a$ for *smaller* clusters $n$. Specifically, the stealthy direct attack achieves a higher $P_a$ than the active communications attack for $n \leq 20$ for $p = 0.1$ and for $n \leq 40$ for $p = 0.05$. For higher values of $n$, the stealth condition $\mathcal{S}$ dictates that a smaller probability of attack $q^*$ must be utilized as shown in Section C. Thus the $P_a$ of the direct stealthy attack tapers off

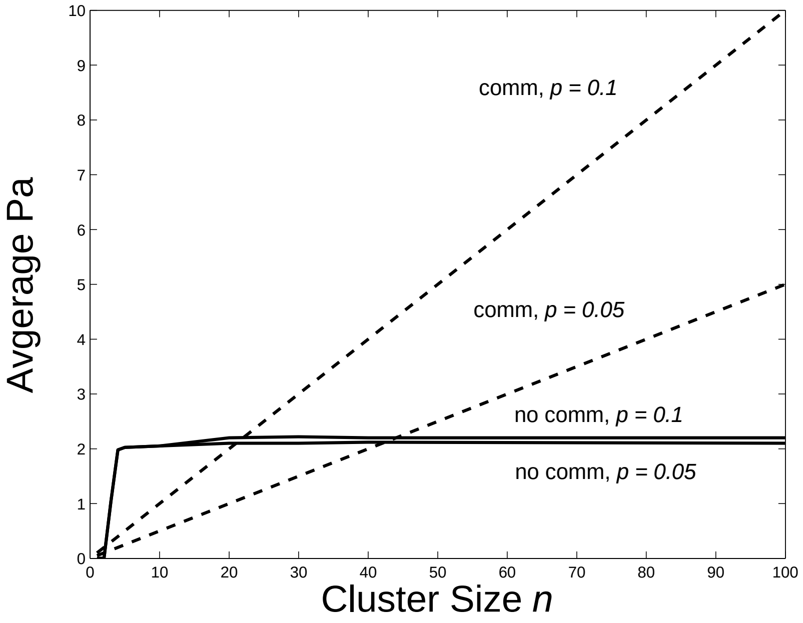


Fig. 26. Comparison of the power of the attack $P_a$ for various cluster sizes $n$ and probabilities $p$ for the direct stealth attack (no communications) and the active communications attack.

in tandem with increasing $n$. Interestingly, this gives rise to the phenomenon of an almost *constant* level of $P_a$ over $n$. Thus if examined by the legitimate network, this constant “background” level of “error” could be mistaken for an inherent probability of a fault associated with the sensor technology. The direct stealthy attack thus exhibits stealth over the size of the cluster $n$. In contrast, the active communications attack allows the entire hostile network to organize itself to meet the stealth condition perfectly. Thus in the active communications attack, the hostile network is able to keep increasing the power of the attack as the cluster size $n$ increases. Finally we note that as predicted in the analysis of Sections C and D, smaller values of probability $p$ favor the legitimate network by restricting the power of the attack that maintains stealth.

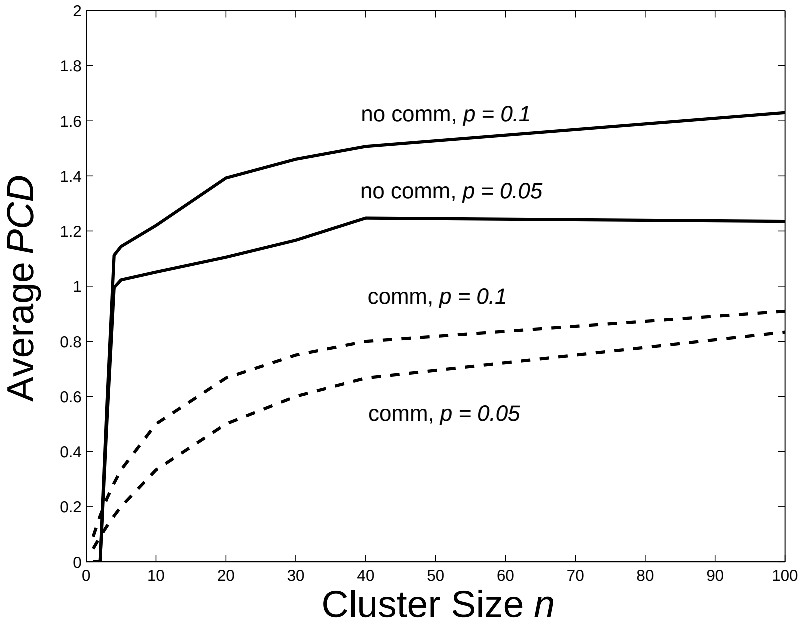


Fig. 27. Comparison of the $PCD$ metric for various cluster sizes $n$ and probabilities $p$ for the direct stealth attack (no communications) and the active communications attack.

Based on Figure 26 we conclude that the direct stealthy attack achieves a higher $P_a$ for smaller clusters $n$ and that the active communications attack achieves higher values of $P_a$ for larger clusters $n$. The former attack may not always achieve perfect stealth since it relies on coordination alone while the latter attack requires active communication. We thus compare the two attacks in terms of their power-communication-detection $PCD$ metrics as shown in Figure 27.

As can be seen from Figure 27, once the number of required communications and the probability of attack detection $P_D$ at the cluster head are also factored into the comparison, the direct stealthy attack achieves a superior $PCD$ performance for $n \geq 2$ for all values of probability $p$. This result is predominantly due to the increasing number of required communications which grow in an affine manner with increasing $n$.

This outcome is significant since the *minimum* number of required communications was utilized for the comparison thus presenting a best case scenario for the active communications attack. We thus conclude that for very small clusters, the active communications attack produces a very small $PCD$ advantage over the direct stealthy attack. For larger clusters the communication overhead may be prohibitive and thus favors the direct stealthy attack. Overall we conclude that the appeal of the direct stealthy attack stems from three properties as compared with active communication: 1- it achieves a higher $P_a$ for $n \leq 20$, 2- it achieves a higher $PCD$ over almost the entire range of $n$ and 3- it exhibits a constancy in $P_a$ over $n$ that may be mistaken for inherent sensor faults.

Finally we make a brief but important observation regarding the implementability of a stealthy hostile attack under the active communications paradigm. Namely, we note that based on the stealth condition $\mathcal{S}$, the active communication attack is indeed implementable for the hostile nodes from a game theoretic perspective without the need for special enforcement. We demonstrate this point through a leader-follower example. In this example, the hostile node that communicates first is called the leader and it announces to the follower its choice of attack parameter. As shown in Figure 28, the second node's (the follower's) optimal action is to always *match* the action of the first node in order to maximize its stealth utility. Thus the attack is implementable in the sense that given an announcement from a subset of nodes, the remaining nodes have no incentive to deviate from the strategy dictated by the leaders.

## F. Chapter Summary

In this chapter we investigated the competing networks scenario for the case of a direct stealthy attack perpetrated by a distributed hostile network. In the direct stealthy

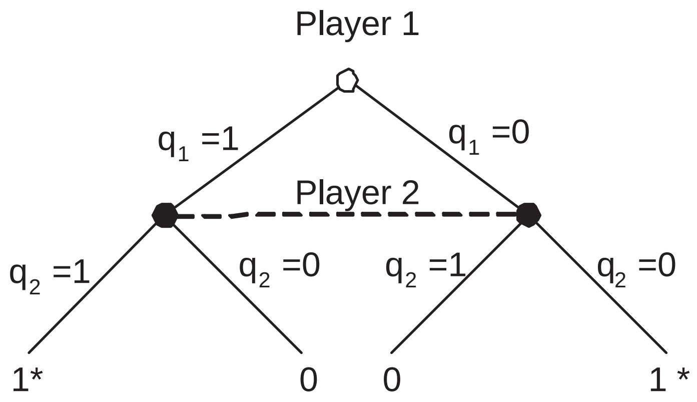


Fig. 28. To maintain stealth, the follower must match the leader.

attack each hostile node may attack a legitimate node with some probability chosen such that the overall stealth of the hostile network is maintained. The persistence and pervasiveness of the attack throughout the cluster causes incorrect individual sensor decisions as well as errors in the collective decision at the cluster head. Attack detection and mitigation are made challenging by the distributed nature of the attacker, the occurrence of the attack at the physical sensing layer and the lack of knowledge concerning the specific actions of the attacker a priori.

The competitive interaction between the two networks is modeled as a game $\mathcal{G}$ where we derive a stealth condition $\mathcal{S}$ and show its consistency and relevance for both the hostile and the legitimate network in terms of attack detection and mitigation. For the hostile network H we show how the stealth condition can be utilized to select the optimal attack parameter for cases where the cluster size $n$ and the sensor threshold $T_h$ of the legitimate network L may not be known. For the legitimate network L we show how the stealth condition yields the optimal defense parameters in terms of $n$ and $T_h$ and how this analysis enables the use of established detection tools such as the Neyman-Pearson paradigm. In general, the optimal attack parameter decreases with increasing cluster size $n$ and with decreasing probability of an event $p$. While this improves attack mitigation by restricting the power of the attack $P_a$, it also makes the attack less detectable at the cluster head and thus presents a detection-mitigation trade-off for the legitimate network.

The direct stealthy attack does not require active communication among the hostile nodes during the attack but rather depends on a level of coordination which we quantify. Compared with the active communications case, we show that the stealthy direct attack achieves a higher power of attack $P_a$ for $n \leq 20$ and a higher power-communication-detection $PCD$ metric for $n \geq 2$. Importantly, the direct stealthy attack exhibits a constancy in $P_a$ over $n$ that may be mistaken for inherent sensor faults and is thus highly desirable for stealth.

Finally we note the role that encryption plays in the competing networks scenario. Forward encryption between the sensors and the sink cannot protect against a hostile attack due to its occurrence during data collection. Based on the role of the sensor threshold $T_h$ in the stealth game, it is the backward encryption between the sink and the sensors that plays a role in attack mitigation and discovery.

# CHAPTER IV

# STEALTHY CROSS COMPETITION*

## A. Introduction and Motivation

In this chapter we investigate the competing sensor networks scenario for the case of a stealthy cross attack. In a stealthy cross attack, each hostile node may attack one or more legitimate nodes with some probability, causing an incorrect decision at the sensor. Unlike in the direct stealthy attack however, based on hostile node deployment and goals, two hostile nodes may both attack the same legitimate node. The cross attack can cause errors in both the local sensor decisions and in the collective sensor decision at the cluster head with ramifications for data acquisition. It is not clear however if the cross attack is more beneficial to the hostile network in terms of attack power and stealth than the direct attack, or if the cross attack creates a form of interference among the attackers that benefits the legitimate network by lowering the attacker's performance.

To examine the ramifications of the cross attack for both the hostile and the legitimate network, we model the interaction between the hostile nodes as a static non-cooperative game. We derive the stealth utility for this scenario and show that it is consistent for both the hostile and the legitimate networks. Based on the stealth utility, the optimal attack and defense strategies are obtained for each network. For the hostile network, we show that surprisingly there exist strategies for the cross attack that achieve superior stealth for H than the direct stealthy attack without the

*Part of the material in this chapter is reprinted with permission from A. Czarlinska and D. Kundur, "Reliable Scalar-Visual Event-Detection in Wireless Visual Sensor Networks," in *Proc. IEEE Consumer Communications & Networking Conference Special Session on Image/Video Processing & Wireless Sensor Networks*, Las Vegas, Nevada, January 2008, pp. 660–664. © 2008 IEEE.

need for communication. Furthermore there exists a unique attack strategy in the cross attack which results in a superior power-communication-detection metric than the direct attack.

For the legitimate network, we employ the derived stealth condition to obtain the best defense strategies. We show how the cross attack presents a greater challenge for L than the direct attack in terms of attack detection for both the optimal and sub-optimal versions of the detector in the Neyman-Pearson paradigm. We demonstrate however how analysis of the attack enables use of these established detection techniques and produces a detection performance that agrees with the predictions of the stealth condition.

## B. System Model

We consider two competing sensor networks deployed in a common environment. Based on deployment and goals, each hostile node may attack one or more legitimate sensors with some probability. For analytical tractability of the cross attack, we focus on a subset of the cluster's nodes. That is we focus on the case of two hostile nodes $h_1$ and $h_2$ deployed in the vicinity of two legitimate sensors $l_1$ and $l_2$ as shown in Figure 29.

As in the case of the direct stealthy attack, the data acquisition model of each sensor is given by Eq. (4.1) and the resulting sensors decisions $x_i$ are modeled as Bernoulli random variables with distribution $X_i \sim Bern(p)$. In this context, $\mathbf{x}$ denotes the decision vector received from the sensors by the cluster head as given in Eq. (4.2).

$$x_i = \gamma_(o_i) = \mathbb{I}_{\{o_i \geq Th\}} \quad \text{s.t} \quad p = \int_{Th}^{\infty} f_0(\alpha) d\alpha \tag{4.1}$$

Each hostile node $h_i$ may attack one or both of the legitimate sensors $l_1$ and $l_2$

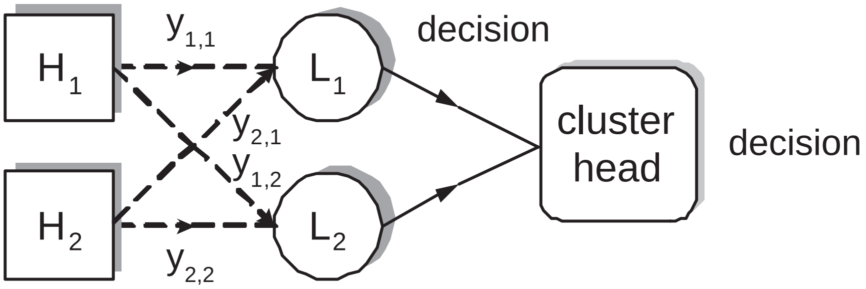


Fig. 29. Stealthy cross attack model.

with some probability. The realization of the attack of hostile node $h_i$ is denoted by $\mathbf{y_i} = [y_{i,1}, y_{i,2}]$ where $y_{i,1}$ denotes the attack of $h_i$ on the legitimate sensor $l_1$ and where $y_{i,2}$ denotes $h_i$'s attack on the legitimate sensor $l_2$ as given in Eqs. (4.3) and (4.4).

$$\mathbf{x} = [x_1, x_2] \qquad x_i \in \{0,1\} \tag{4.2}$$

$$\mathbf{y_1} = [y_{1,1}, y_{1,2}] \quad y_{1,i} \in \{0,1\} \tag{4.3}$$

$$\mathbf{y_2} = [y_{2,1}, y_{2,2}] \quad y_{2,i} \in \{0,1\} \tag{4.4}$$

More specifically, the cross attack enables each hostile node to choose one of four possible attack vectors $\mathbf{y_i}$. That is, each hostile node $h_i$ may attack neither $l_1$ nor $l_2$, attack $l_1$ but not $l_2$, attack $l_2$ but not $l_1$ or attack both $l_1$ and $l_2$. For each hostile node $h_i$, each of these four attack vectors is defined as shown in Eqs. (4.5) to (4.8).

$$a \triangleq [y_{1,1}, y_{1,2}] = [0,0], \quad \tilde{a} \triangleq [y_{2,1}, y_{2,2}] = [0,0] \tag{4.5}$$

$$b \triangleq [y_{1,1}, y_{1,2}] = [0,1], \quad \tilde{b} \triangleq [y_{2,1}, y_{2,2}] = [0,1] \tag{4.6}$$

$$c \triangleq [y_{1,1}, y_{1,2}] = [1,0], \quad \tilde{c} \triangleq [y_{2,1}, y_{2,2}] = [1,0] \tag{4.7}$$

$$d \triangleq [y_{1,1}, y_{1,2}] = [1,1], \quad \tilde{d} \triangleq [y_{2,1}, y_{2,2}] = [1,1] \tag{4.8}$$

To perpetrate a stealthy attack based on the possible attack vectors, each hostile node must thus assign an optimal attack probability to each possible attack vector as shown in Eqs. (4.9) to (4.12). Thus the action set of hostile node $h_1$ consists of an assignment of attack probabilities $\mathbf{q} = [q_1, q_2, q_3, q_4]$ where $\Sigma_{i=1}^{4} q_i = 1$ as shown in Eq. (4.14). Similarly, the action set of hostile node $h_2$ consists of an assignment of probabilities $\tilde{\mathbf{q}} = [\tilde{q}_1, \tilde{q}_2, \tilde{q}_3, \tilde{q}_4]$ where $\Sigma_{i=1}^{4} \tilde{q}_i = 1$ as shown in Eq. (4.15).

$$Pr\{a\} \triangleq q_1 \quad Pr\{\tilde{a}\} \triangleq \tilde{q}_1 \tag{4.9}$$

$$Pr\{b\} \triangleq q_2 \quad Pr\{\tilde{b}\} \triangleq \tilde{q}_2 \tag{4.10}$$

$$Pr\{c\} \triangleq q_3 \quad Pr\{\tilde{c}\} \triangleq \tilde{q}_3 \tag{4.11}$$

$$Pr\{d\} \triangleq q_4 \quad Pr\{\tilde{d}\} \triangleq \tilde{q}_4 \tag{4.12}$$

$$\Sigma_{i=1}^{4} q_i = 1 \quad \Sigma_{i=1}^{4} \tilde{q}_i = 1 \tag{4.13}$$

$$\mathbf{q} = [q_1, q_2, q_3, q_4] \tag{4.14}$$

$$\tilde{\mathbf{q}} = [\tilde{q}_1, \tilde{q}_2, \tilde{q}_3, \tilde{q}_4] \tag{4.15}$$

The effect of the attack upon the decisions of the sensor nodes is modeled via Eq. (4.16). In Eq. (4.16), $\mathbf{X}$ is the pristine data vector when the cross attack is not present, $\mathbf{Y_1}$ is the attack vector of hostile node $h_1$, $\mathbf{Y_2}$ is the attack vector of hostile node $h_2$ and $\oplus$ is modulo 2 addition.

$$\mathbf{Z} = \mathbf{X} \oplus \mathbf{Y_1} \oplus \mathbf{Y_2} \tag{4.16}$$

Based on the attack model of Eq. (4.16) and the goal of the hostile network to misguide the legitimate network while minimizing the chance of attack detection, we obtain the requirement for stealth as given by definition 4. Importantly, the stealth condition $\mathcal{S}_c$ for the cross attack defined in Eq. (4.17) depends on the probability $p$ of an event (which depends on the underlying threshold $T_h$ selection at the sensors), as well as on the attack selections $\mathbf{q}$ and $\tilde{\mathbf{q}}$ of *each* hostile nodes.

**Definition 4** *The stealth condition $\mathcal{S}_c$ of the hostile sensor network $H$ for the cross attack is given by Eq. (4.17) where $w$ is the weight of a vector and is defined as $w(\xi) \doteq \sum_{i=1}^{n} \xi_i$ for a vector $\xi$ of length $n$.*

$$\mathcal{S}_c = Pr\{w(\mathbf{Z}_{p,q,\tilde{q}}) = w(\mathbf{X}_p)\} \tag{4.17}$$

The interactions between the two hostile nodes $h_1$ and $h_2$ with consequences for the legitimate network L are modeled as a static non-cooperative game $\mathcal{G}_c$ as given by definition 5. Importantly, the interaction between the hostile nodes in $\mathcal{G}_c$ is non-cooperative in the game theoretic sense signifying that the hostile nodes do not utilize any form of binding or enforceable contract between them in order to reach the common stealth goal. Rather, each hostile node $h_i$ selects an action from its action set $A_i$ to achieve maximal stealth utility $u_i(p, \mathbf{q}, \tilde{\mathbf{q}})$ while choosing this action independently of the other hostile node.

**Definition 5** *The stealthy cross game is given by:*

$$\mathcal{G}_c = \langle \Gamma, A, U \rangle = \langle \{h_1, h_2\}, \{A_1, A_2\}, \{u_1, u_2\} \rangle \tag{4.18}$$

$$A_1 = \{\mathbf{q} : \Sigma_{i=1}^{4} q_i = 1\} \quad A_2 = \{\tilde{\mathbf{q}} : \Sigma_{i=1}^{4} \tilde{q}_i = 1\} \tag{4.19}$$

$$u_1(p, \mathbf{q}, \tilde{\mathbf{q}}) = u_2(p, \mathbf{q}, \tilde{\mathbf{q}}) = Pr\{w(\mathbf{Z}_{p,q,\tilde{q}}) = w(\mathbf{X}_p)\} \tag{4.20}$$

To solve the cross attack game and obtain the optimal actions of each hostile node, we are looking for best response functions $B_1(\tilde{\mathbf{q}}^*)$ and $B_2(\mathbf{q}^*)$ where the notation $B_a(b)$ denotes the best response $B$ of player $a$ to the opponents best strategy $b$ as given by Eqs. (4.21) and (4.22) respectively.

$$B_1(\tilde{\mathbf{q}}^*) = \text{arg max} \quad {}_{\mathbf{q}:\Sigma_{i=1}^{4} q_i = 1} \quad Pr\{w(\mathbf{Z}_{p,q,\tilde{q}}) = w(\mathbf{X}_p)\} \tag{4.21}$$

$$B_2(\mathbf{q}^*) = \text{arg max} \quad {}_{\tilde{\mathbf{q}}:\Sigma_{i=1}^{4} \tilde{q}_i = 1} \quad Pr\{w(\mathbf{Z}_{p,q,\tilde{q}}) = w(\mathbf{X}_p)\} \tag{4.22}$$

## C. Stealthy Attack Results

In this section we analyze and solve the cross stealthy attack game $\mathcal{G}_c$ from definition 5. We begin by obtaining the stealth condition $\mathcal{S}_c$ from Eq. (4.17) and by defining the notion of pure and mixed actions of the hostile nodes in the game $\mathcal{G}_c$ as they pertain to the solution of the cross stealthy attack problem.

**Definition 6** *An action* $\mathbf{q}$ *of hostile node* $h_1$ *where* $\mathbf{q} = [q_1, q_2, q_3, q_4]$ *is an assignment of probabilities* $q_1$*,* $q_2$*,* $q_3$ *and* $q_4$ *such that* $\Sigma_{i=1}^{4} q_i = 1$ *and* $q_1, q_2, q_3, q_4 > 0$*. Similarly an action* $\tilde{\mathbf{q}}$ *of hostile node* $h_2$ *is an assignment of probabilities* $\tilde{q}_1$*,* $\tilde{q}_2$*,* $\tilde{q}_3$ *and* $\tilde{q}_4$ *such that* $\Sigma_{i=1}^{4} \tilde{q}_i = 1$ *and* $\tilde{q}_1, \tilde{q}_2, \tilde{q}_3, \tilde{q}_4 > 0$*.*

**Definition 7** *A pure action* $\mathbf{q_{Pk}}$ *(or* $\tilde{\mathbf{q}}_{\mathbf{Pk}}$*) is an assignment of probabilities* $q_1$*, ...,* $q_4$ *(or* $\tilde{q}_1$*, ...,* $\tilde{q}_4$*) such that the* $k$*th element carries probability* 1 *and the remaining elements carry probability* 0*. For instance,* $\mathbf{q_{P1}}$ *is the pure action vector* $[q_1, q_2, q_3, q_4] = [1, 0, 0, 0]$ *and* $\tilde{\mathbf{q}}_{\mathbf{P3}}$ *is the pure action vector* $[\tilde{q}_1, \tilde{q}_2, \tilde{q}_3, \tilde{q}_4] = [0, 0, 1, 0]$*.*

**Definition 8** *A mixed action* $\mathbf{q_M} = [q_1, q_2, q_3, q_4]$ *(or* $\tilde{\mathbf{q}}_{\mathbf{M}} = [\tilde{q}_1, \tilde{q}_2, \tilde{q}_3, \tilde{q}_4]$*) is an assignment of probabilities that is* not *a pure action. For example,* $[q_1, q_2, q_3, q_4] = [0.5, 0, 0.5, 0]$ *is a mixed action as is* $[\tilde{q}_1, \tilde{q}_2, \tilde{q}_3, \tilde{q}_4] = [0.25, 0.25, 0.25, 0.25]$*.*

**Example 1** *An action* $\mathbf{q} = [0.25, 0.75, 0, 0]$ *signifies that hostile node* $h_1$ *will actuate according to strategy* $a$ *as defined in Eq. (4.5) with probability* 0.25 *and according to strategy* $b$ *as defined in Eq. (4.6) with probability* 0.75*. This is thus a mixed strategy on the part of* $h_1$*.*

We proceed to obtain the stealth condition $\mathcal{S}_c$ for the cross attack by expressing it in terms of the underlying probabilities as shown in Eqs. (4.23) and (4.24) with the result of the simplification shown via Eq. (4.25) to Eq. (4.29).

$$\begin{aligned}\mathcal{S}_c = Pr\{w(\mathbf{Z}_{p,q,\tilde{q}}) = w(\mathbf{X}_p)\} = & Pr\{w(\mathbf{X}_p) = w(\mathbf{Z}_{p,q,\tilde{q}})|\mathbf{X} = 00\} \cdot Pr\{\mathbf{X} = 00\} \\ & + Pr\{w(\mathbf{X}_p) = w(\mathbf{Z}_{p,q,\tilde{q}})|\mathbf{X} = 01\} \cdot Pr\{\mathbf{X} = 01\} \\ & + Pr\{w(\mathbf{X}_p) = w(\mathbf{Z}_{p,q,\tilde{q}})|\mathbf{X} = 10\} \cdot Pr\{\mathbf{X} = 10\} \\ & + Pr\{w(\mathbf{X}_p) = w(\mathbf{Z}_{p,q,\tilde{q}})|\mathbf{X} = 11\} \cdot Pr\{\mathbf{X} = 11\} \end{aligned} \quad (4.23)$$

$$\begin{aligned}\mathcal{S}_c = (q_1\tilde{q}_1 + q_2\tilde{q}_2 + q_3\tilde{q}_3 + q_4\tilde{q}_4) \cdot (1-p)^2 + 2p(1-p) \cdot \\ (q_1\tilde{q}_1 + q_2\tilde{q}_2 + q_3\tilde{q}_3 + q_4\tilde{q}_4 + q_2\tilde{q}_3 + q_3\tilde{q}_2 + q_4\tilde{q}_1 + q_1\tilde{q}_4) + \\ p^2 \cdot (q_1\tilde{q}_1 + q_2\tilde{q}_2 + q_3\tilde{q}_3 + q_4\tilde{q}_4) \end{aligned} \quad (4.24)$$

$$\mathcal{S}_c \quad = \alpha\beta_p + \delta_p(\alpha + \gamma) \quad (4.25)$$

$$\alpha \quad = q_1\tilde{q}_1 + q_2\tilde{q}_2 + q_3\tilde{q}_3 + q_4\tilde{q}_4 \quad (4.26)$$

$$\gamma \quad = q_2\tilde{q}_3 + q_3\tilde{q}_2 + q_4\tilde{q}_1 + q_1\tilde{q}_4 \quad (4.27)$$

$$\beta_p \quad = 1 - 2p + 2p^2 \quad (4.28)$$

$$\delta_p \quad = 2p(1-p) \quad (4.29)$$

We note however that that the terms $\beta_p$ and $\delta_p$ obey the relationship $\beta_p + \delta_p = 1$ thus leading to the simplification shown in Eq. (4.30) where $u_i$ is the stealth utility of each hostile node $h_i$.

$$\mathcal{S}_c = u_i(p, \mathbf{q}, \tilde{\mathbf{q}}) = \alpha + \gamma \cdot \delta_p \qquad \delta_p \in [0, 0.5], \quad i \in \{1, 2\} \quad (4.30)$$

### 1. Attack Analysis

Based on the stealth condition $\mathcal{S}_c$ from Eq. (4.30) we set out to identify the optimal actions of each hostile node that result in the maximization of the stealth condition.

**Proposition 1** *The best response of a hostile node $h_i$ to a pure action of hostile node $h_j$ in the stealthy cross attack game $\mathcal{G}_c$ is a* matching *pure action. That is,*

$$\begin{aligned} B_1(\tilde{\mathbf{q}}_{\mathbf{Pk}}) &= \mathbf{q}_{\mathbf{Pk}} \\ B_2(\mathbf{q}_{\mathbf{Pk}}) &= \tilde{\mathbf{q}}_{\mathbf{Pk}} \end{aligned} \tag{4.31}$$

*The four resulting pure action Nash equilibria are thus given by Eq. (4.32) where the subscript $N$ denotes a Nash equilibrium.*

$$(\mathbf{q}_{\mathbf{N}}, \tilde{\mathbf{q}}_{\mathbf{N}}) = (\mathbf{q}_{\mathbf{Pk}}, \tilde{\mathbf{q}}_{\mathbf{Pk}}) \quad k \in \{1, 2, 3, 4\} \tag{4.32}$$

*The resulting utility $u_i$ for hostile node $h_i \in \{1, 2\}$ is given by Eq. (4.33)*

$$u_i(\mathbf{q}_{\mathbf{N}}, \tilde{\mathbf{q}}_{\mathbf{N}}) = 1 \tag{4.33}$$

**Proof 11** *We note that the utilities for hostile nodes $h_1$ and $h_2$ given by $u_1$ and $u_2$ from Eq. (4.30) can be re-written as shown in Eq. (4.34) and (4.35) where the dependence on probability $p$ is not emphasized explicitly in the notation.*

$$\begin{aligned} u_1(\mathbf{q}, \tilde{\mathbf{q}}) &= q_1(\tilde{q}_1 + \delta_p \tilde{q}_4) \\ &+ q_2(\tilde{q}_2 + \delta_p \tilde{q}_3) \\ &+ q_3(\tilde{q}_3 + \delta_p \tilde{q}_2) \\ &+ q_4(\tilde{q}_4 + \delta_p \tilde{q}_1) \end{aligned} \tag{4.34}$$

$$\begin{aligned} u_2(\mathbf{q}, \tilde{\mathbf{q}}) &= \tilde{q}_1(q_1 + \delta_p q_4) \\ &+ \tilde{q}_2(q_2 + \delta_p q_3) \\ &+ \tilde{q}_3(q_3 + \delta_p q_2) \\ &+ \tilde{q}_4(q_4 + \delta_p q_1) \end{aligned} \tag{4.35}$$

*Based on Eq. (4.34), a pure strategy* $\mathbf{q_{Pk}}$ *by* $h_1$ *results in utility* $u_2 = \tilde{q}_k + \delta_p \tilde{q}_m$ *for hostile node* $h_2$ *where* $m \in \{1,2,3,4\}$ excludes $k \in \{1,2,3,4\}$*. The proof is completed by noticing that* $\delta_p \in [0, 0.5]$*. Therefore given any pure action* $q_{Pk}$*, the best response of node* $h_2$ *is to match with a pure strategy of the same value of* $k$*. This results in a utility of* $1$ *for each player. Similarly based on Eq. (4.35), given any pure action* $\tilde{q}_{Pk}$*, node* $h_1$ *faces a utility* $u_1 = q_k + \delta_p q_m$ *where* $m \in \{1,2,3,4\}$ excludes $k \in \{1,2,3,4\}$*. Thus the best response of node* $h_1$ *is to match the pure action with the same* $k$*.*

**Example 2** *Suppose that node* $h_1$ *plays with pure action* $\mathbf{q_{P2}} = [0,1,0,0]$*. Hostile node* $h_2$ *thus faces the following utility* $u_2 = \tilde{q}_1(0 + \delta_p 0) + \tilde{q}_2(1 + \delta_p 0) + \tilde{q}_3(0 + \delta_p 1) + \tilde{q}_4(0 + \delta_p 0) = \tilde{q}_2 + \delta_p \tilde{q}_3$*. Since* $\delta_p \in [0, 0.5]$*, the unique best response choice is to set* $\tilde{q}_2 = 1$*. Given the choice of* $\tilde{q}_2 = 1$*, hostile node* $h_1$ *has no incentive to deviate from its original strategy of* $q_2 = 1$ *since it faces the utility* $u_1 = q_1(0 + \delta_p 0) + q_2(1 + \delta_p 0) + q_3(0 + \delta_p 1) + q_4(0 + \delta_p 0) = q_2 + \delta_p q_3$*.*

In general we can conclude that a choice of a pure strategy by one of the hostile nodes induces a matching pure strategy in the second hostile node.

**Proposition 2** *A mixed strategy equilibrium exists in the stealthy cross attack game* $\mathcal{G}_c$ *iff the following two conditions are satisfied:*

1. *Player* $1$ *assigns equal probabilities* $q_i = k$ *to the non-zero components of his action vector.*
2. *Player* $2$ *assigns the same equal probabilities to his action vector as player* $1$*.*

*This leads to the existence of multiple mixed equilibria with varying utilities* $u_i < 1$ *for* $i \in \{1, 2\}$*.*

**Proof 12** *Let* $I = \{i \in \{1,2,3,4\} : q_i \neq 0\}$ *and let* $k = 1/|I|$ *where* $|\cdot|$ *denotes the* *cardinality of the set. Without loss of generality, assume that player* 1 *is hostile node* $h_1$ *and that player* 2 *is hostile node* $h_2$*.*

*We begin by considering the case where* $|I| = 4$*, that is, there are no elements with assigned probability of* 0 *in the action vector. In this case, the equal probability assignment (requirement* 1*) results in the action vector of* $h_1$ *given by* $\mathbf{q_M} = [q_1, q_2, q_3, q_4] = [k, k, k, k]$ *where* $k = 1/4$*. This assignment results in a utility for* $h_2$ *given by* $u_2 = \tilde{q}_1(k+\delta_p k)+\tilde{q}_2(k+\delta_p k)+\tilde{q}_3(k+\delta_p k)+\tilde{q}_5(k+\delta_p k) = k(1+\delta_p)(\tilde{q}_1+\tilde{q}_2+\tilde{q}_3+\tilde{q}_4)$*. Since* $\Sigma_{1=1}^{4}\tilde{q}_i = 1$*, we note that any distribution of probabilities among the* $\tilde{q}_i$*'s results in a utility* $u_2 = k(1+\delta_p) = 1/4 \cdot (1+\delta_p)$*. Thus* $h_2$ *is indifferent between his/her mix of probability assignments* $\tilde{\mathbf{q}}_{\mathbf{M}}$*.*

*However we observe that only the mix* $\tilde{\mathbf{q}}_{\mathbf{M}} = [1/4, 1/4, 1/4, 1/4]$ *results in a mixed Nash* equilibrium*. To see this, assume that at least one of the* $\tilde{q}_i$ *assignments is larger than the others. For example,* $\tilde{q}_1$ *is larger than the other components, say* $\tilde{\mathbf{q}}_{\mathbf{M}} = [1/2, 1/6, 1/6, 1/6]$*. Then by examining Eq. (4.34), it is easy to see that* $h_1$*'s best response is to alter its mix, setting* $q_1 = 1$ *and* $q_2 = 0$*,* $q_3 = 0$ *and* $q_4 = 0$*. This action in turn induces* $h_2$*'s best response* $\tilde{q}_1 = 1$*. The only stable situation leading to a mixed strategy Nash equilibrium is the one where player* 2 *matches the equal distribution of player* 1*. If these conditions are not met, the situation degenerates to a pure strategy Nash equilibrium. The proof for* $|I| = 3$*,* 2 *and* 1 *follows the same methodology though the case of* $|I| = 3$ *deserves further mention due the interesting role of* $\delta_p$*.*

*For the* $|I| = 3$ *case, assume without loss of generality that* $q_1 = q_2 = q_3 = 1/3$ *and that* $q_4 = 0$*. The resulting utility* $u_1$ *faced by node* $h_1$ *is thus* $u_2 = 1/3 \cdot \tilde{q}_1 + 1/3 \cdot (1+\delta_p)\tilde{q}_2 + 1/3 \cdot (1+\delta_p)\tilde{q}_3 + 1/3 \cdot \delta_p\tilde{q}_4$*. If* $\delta_p = 0$*,* $u_2 = 1/3 \cdot \tilde{q}_1 + 1/3 \cdot \tilde{q}_2 + 1/3 \cdot \tilde{q}_3$*. Thus player* $h_2$ *is indifferent between allocations to* $\tilde{q}_1$*,* $\tilde{q}_2$ *and* $\tilde{q}_3$*. An allocation of* $\tilde{q}_1 = \tilde{q}_2 = \tilde{q}_3$ *results in a mixed equilibrium. An allocation of* $\tilde{q}_1 > \tilde{q}_2 > \tilde{q}_3$ *results in* *a degeneration to a pure strategy involving* $q_1$ *and* $\tilde{q}_1$*. An allocation of* $\tilde{q}_1 = \tilde{q}_2 > \tilde{q}_3$ *results in a degeneration to a mixed equilibrium involving equal mixing between* $q_1$ *and* $q_2$ *for* $h_1$ *and* $\tilde{q}_1$ *and* $\tilde{q}_2$ *for* $h_2$*. However an interesting development occurs when* $\delta_p \neq 0$ *in* $u_2 = 1/3 \cdot \tilde{q}_1 + 1/3 \cdot (1+\delta_p)\tilde{q}_2 + 1/3 \cdot (1+\delta_p)\tilde{q}_3 + 1/3 \cdot \delta_p \tilde{q}_4$*. For any value of* $\delta_p \in [0, 0.5]$*,* $1/3 \cdot (1+\delta_p)\tilde{q}_i \geq 1/3 \cdot \tilde{q}_i > 1/3 \cdot \delta_p \tilde{q}_i$*. Therefore the node is only indifferent between* two *and not three of the strategies. In this case* $h_2$ *is indifferent between* $\tilde{q}_2$ *and* $\tilde{q}_3$*. If* $h_2$ *mixes among these actions with equal probability then this case degenerates to* $|I| = 2$*, otherwise it degenerates to* $|I| = 1$*.*

Summary of Results:

- Case $|I| = 4$. There is a unique mixed Nash strategy equilibrium at $(\mathbf{q_P}, \tilde{\mathbf{q}}_\mathbf{P})$ where $\mathbf{q_P} = \tilde{\mathbf{q}}_\mathbf{P} = [k, k, k, k]$ with $k = 1/4$. The associated relative stealth utility $u_i = 1/4 \cdot (1+\delta_p)$ for all $i \in [1, 2]$.

- Case $|I| = 3$. If $\delta_p = 0$ (which corresponds to the case of $p = 0$ or $p = 1$), there are four mixed Nash strategy equilibria for this case where there is a single zero component in an action vector. These are given by: $\mathbf{q_P} = \tilde{\mathbf{q}}_\mathbf{P} = [0, k, k, k]$, $\mathbf{q_P} = \tilde{\mathbf{q}}_\mathbf{P} = [k, 0, k, k]$, $\mathbf{q_P} = \tilde{\mathbf{q}}_\mathbf{P} = [k, k, 0, k]$ and $\mathbf{q_P} = \tilde{\mathbf{q}}_\mathbf{P} = [k, k, k, 0]$ for $k = 1/3$. If however $\delta_p \neq 0$, no mixed equilibria exist in this case. Indeed in the presence of $\delta_p$, the pure equilibria reduce to those for the case of $|I| = 2$. In the case where the triplet does exist, the associated relative stealth utility $u_i = 1/3 \cdot (1 + 2/3 \cdot \delta_p)$ for all $i \in [1, 2]$.

- Case $|I| = 2$. There are six mixed Nash strategy equilibria for this case with two zero components in an action vector. These are given by $\mathbf{q_P} = \tilde{\mathbf{q}}_\mathbf{P} = [k, 0, 0, k]$, $\mathbf{q_P} = \tilde{\mathbf{q}}_\mathbf{P} = [0, k, k, 0]$, $\mathbf{q_P} = \tilde{\mathbf{q}}_\mathbf{P} = [k, k, 0, 0]$, $\mathbf{q_P} = \tilde{\mathbf{q}}_\mathbf{P} = [0, 0, k, k]$, $\mathbf{q_P} = \tilde{\mathbf{q}}_\mathbf{P} = [k, 0, k, 0]$ and $\mathbf{q_P} = \tilde{\mathbf{q}}_\mathbf{P} = [0, k, 0, k]$ with $k = 1/2$. Based on the structure of the stealth condition, the first two doublets result in a relative stealth utility $u_i = 1/2 \cdot (1 + \delta_p)$ for all $i \in [1, 2]$. The remaining doublets result in a relative stealth utility $u_i = 1/2$ for all $i \in [1, 2]$. Thus the average utility experienced by the hostile nodes while carrying out a doublet attack is given by $\bar{u}_i = 1/2 \cdot (1 + 1/3 \cdot \delta_p)$ for all $i \in [1, 2]$.

- Case $|I| = 1$. This case is the pure strategy case. There are four pure strategy Nash equilibria for this case of three zero components in an action vector. These are given by $\mathbf{q_P} = \tilde{\mathbf{q}}_\mathbf{P} = [k, 0, 0, 0]$, $\mathbf{q_P} = \tilde{\mathbf{q}}_\mathbf{P} = [0, k, 0, 0]$, $\mathbf{q_P} = \tilde{\mathbf{q}}_\mathbf{P} = [0, 0, k, 0]$ and $\mathbf{q_P} = \tilde{\mathbf{q}}_\mathbf{P} = [0, 0, 0, k]$ where $k = 1$. The associated relative stealth utility $u_i = 1$ for all $i \in [1, 2]$.

Thus based on analysis of the stealth condition $\mathcal{S}_c$ we have obtained the optimal actions of each hostile node which are chosen independently of the other hostile node. In the next section we investigate the significance of these results for the hostile network.

### 2. Attack Performance

In this section we investigate the performance implications of the optimal attack strategies of each hostile node with special emphasis on the role of pure and mixed actions and their effect on the stealth and power of the attack.

We begin by observing that unlike in the direct stealthy attack, the optimal choice of each hostile node is not unique even if each node is restricted to the selection of only pure equilibria. That is, based on the results of proposition 1, there are four possible pure Nash equilibria given by $(\mathbf{q_N}, \tilde{\mathbf{q}}_\mathbf{N}) = (\mathbf{q_{Pk}}, \tilde{\mathbf{q}}_\mathbf{Pk})$ for $k \in \{1, 2, 3, 4\}$. Based on these pure equilibria, to maximize the stealth utility $\mathcal{S}_c$ the hostile nodes must attack with the same attack vector. For the $k = 1$ pure equilibrium attack for instance, *both*

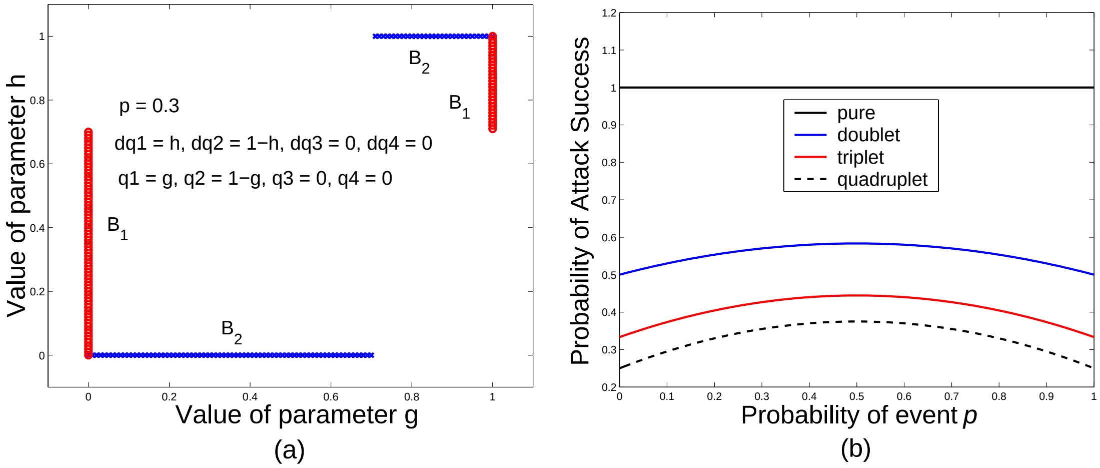


Fig. 30. (a) Best response functions of $h_1$ and $h_2$ showing the emergence of two (out of the possible four) pure equilibria. (b) Comparison of stealth $\mathcal{S}_c$ for various strategy types.

hostile nodes must not attack $l_1$ or $l_2$. For the $k = 4$ pure equilibrium attack, both hostile nodes must attack $l_1$ and $l_2$. This result is illustrated in Figure 30a which depicts a sample case of the best response functions of hostile nodes $h_1$ and $h_2$. In Figure 30a, the actions of hostile node $h_1$ are set to $q_3 = q_4 = 0$, $q_1 = g$ and $q_2 = 1-g$. Thus $h_1$ must select a parameter $g \in [0, 1]$ to achieve the best stealth utility. Hostile node $h_2$ is utilizing actions $\tilde{q}_3 = \tilde{q}_4 = 0$, $\tilde{q}_1 = h$ and $\tilde{q}_2 = 1 - h$. Thus $h_2$ must select a parameter $h \in [0, 1]$ to maximize its stealth utility. As shown in Figure 30a, if $h_1$ chooses $g = 0$, then $h_2$'s optimal choice is to select $h = 0$ and if $h_1$ chooses $g = 1$ then $h_2$'s optimal choice is to select $h = 1$. These two cases of optimal selection lead to the emergence of two of the four pure action Nash equilibria, namely the $(\mathbf{q}, \tilde{\mathbf{q}})$ equilibrium where $\mathbf{q} = [1, 0, 0, 0]$ and $\tilde{\mathbf{q}} = [1, 0, 0, 0]$ and the $(\mathbf{q}, \tilde{\mathbf{q}})$ equilibrium where $\mathbf{q} = [0, 1, 0, 0]$ and $\tilde{\mathbf{q}} = [0, 1, 0, 0]$.

This matching actions result stems directly from the requirement of maximizing the stealth of the hostile network during the attack. However this result carries significant implications for the power of the attack $P_a$ under the pure actions equilibrium which we state in remark 3.

**Remark 3** *The set of pure action equilibria given by* $(\mathbf{q_N}, \tilde{\mathbf{q}}_\mathbf{N}) = (\mathbf{q_{Pk}}, \tilde{\mathbf{q}}_\mathbf{Pk})$ *for* $k \in \{1, 2, 3, 4\}$ *between hostile nodes* $h_1$ *and* $h_2$ *maximize the stealth* $\mathcal{S}_c$ *of the attack achieving the maximal stealth of* $u_i = 1$ *for* $i \in \{1, 2\}$*. However the resulting power of the attack* $P_a$ *stemming from the pure action equilibria yields* $P_a = 0$*. The pure action equilibria of the hostile nodes in the cross stealthy attack thus correspond to the case of interference for the hostile nodes and as such, they are an undesirable attack condition.*

To understand remark 3 we recall that each hostile node actuates in the vicinity of a legitimate node to distort and alter the observation $o_i$ of sensor $i$ regarding the source $O$. In the case of the direct stealthy attack, each hostile node performs the attack in the vicinity of a unique legitimate sensor. However in the cross stealthy attack with pure action equilibria, two hostile nodes are both attacking the same legitimate sensor(s). Each hostile node $i$ thus not only senses the source $O$ but also the actuation created by the other hostile node $j$. Since the goal of each hostile node is to flip the decision of the legitimate sensor (from 1 to 0 and vice versa), each hostile node performs actuation designed to reverse $x_i$ based on the perceived conditions. Thus while hostile node $i$ attempts to flip the decision from $a$ to $b$, hostile node $j$ attempts to flip the decision from $b$ to $a$ resulting in interference and a power of attack $P_a = 0$. The resulting stealth utility of $u_i = 1$ can thus be understood as achieving stealth in the attack by effectively not attacking the decisions of the legitimate network due to interference. From the perspective of the hostile network H, the *pure* action equilibria should thus be avoided. The general trade-off between stealth $\mathcal{S}_c$ and the power of the attack $P_a$ will be further detailed in this section.

Next we wish to consider the role of *mixed* Nash equilibria in attaining stealth and a power of attack. As shown in Section C-1, mixed strategy equilibria are also not unique. Indeed there are three categories or "types" of mixed equilibria: the doublet, the triplet and the quadruplet (the fourth type of equilibrium is the pure equilibrium but it is not a mixed equilibrium). The doublet category for instance includes all the mixed equilibria where each hostile node mixes among two pure actions. Importantly we note that in order to reach a mixed *equilibrium* of the doublet type, each hostile node must utilize the *same* probability mix for its actions as shown in proposition 2. As a counterexample, $\mathbf{q} = [1/2, 1/2, 0, 0]$ and $\tilde{\mathbf{q}} = [1/2, 0, 1/2, 0]$ is not a doublet equilibrium since each node is mixing among different pure actions (although with equal probability). As a second counterexample, $\mathbf{q} = [1/2, 1/2, 0, 0]$ and $\tilde{\mathbf{q}} = [3/4, 1/4, 0, 0]$ is also not an equilibrium since the two nodes are not using the same probability assignment although they are mixing among the same pure actions.

The stealth condition $\mathcal{S}_c$ of Eq. (4.30) predicts the relative level of stealth for all mixed equilibria by equilibrium type as shown in Table II where the heading "Strategy" shows a sample action of hostile node $h_1$ that fits into the given "Strategy Type". We make an important observation regarding the levels of relative stealth shown in Table II. We note that mixing among *fewer* strategies produces a higher relative level of stealth $\mathcal{S}_c$. Specifically, mixing among two strategies is better for the attacker than mixing among three strategies. Mixing among three strategies is in turn better than mixing among four strategies. We note that "mixing" with only one strategy (i.e. employing a pure action) performs best in terms of stealth but corresponds to $P_a = 0$ as discussed in remark 3. This result is depicted in Figure 30b where the stealth $\mathcal{S}_c$ utilities are shown over the entire range of probability $p$ of an event. As can be seen from Figure 30b, the stealth utility improves with a decreased level of mixing and this pattern is maintained over the entire range of probability $p$.

Next we wish to make an important observation regarding the role of the prob-

Table II. Comparison of Stealth Condition for Strategy Types

| Strategy Type | Strategy | Stealth |
|---|---|---|
| pure | $q_1 = 1$ | 1 |
| doublet | $q_1 = q_2 = 1/2$ | $(1/2)(1 + (1/3)\delta_p)$ |
| triplet | $q_1 = q_2 = q_3 = 1/3$ | $(1/3)(1 + (2/3)\delta_p)$ |
| quadruplet | $q_1 = q_2 = q_3 = q_4 = 1/4$ | $(1/4)(1 + \delta_p)$ |

ability $p$ of an event based on the probability density function of the underlying phenomenon and based on the local sensor threshold $T_h$. We observe that as shown in Table II and in Figure 30b, the stealth $\mathcal{S}_c$ utility of each hostile node depends on the parameter $\delta_p$ where $\delta_p = 2p(1-p)$ from Eq. (4.29) and where $\delta_p \in [0, 0.5]$. Since $\delta_p$ achieves its maximal value of $\delta_p = 0.5$ at $p = 0.5$, this is the best case scenario for the hostile H network in terms of relative stealth and conversely the worst case scenario for the legitimate L network. On the other hand, values of probability $p$ that are closest to $p = 0$ or $p = 1$ constitute the best case for the legitimate network. This result is consistent with the direct stealthy attack where the local sensor threshold $T_h$ was set so as to result in a small or large probability $p$ as given in Algorithm 2. Thus we note that the stealth condition $\mathcal{S}_c$ for the cross stealthy attack is consistent for both the legitimate and the hostile network.

Finally we wish to determine the overall performance of the cross stealthy attack in terms of both the resulting stealth $\mathcal{S}_c$ and in terms of the power of attack $P_a$ for the various strategy types. We begin by noting that under the cross attack model of Eq. (4.16), legitimate sensor $l_1$ makes a decision $Z_1$ as given by Eq. (4.36) while legitimate sensor $l_2$ makes a decision $Z_2$ as given by Eq. (4.37).

$$Z_1 = X_1 \oplus Y_{11} \oplus Y_{21} = X_1 \oplus \bar{Y}_1 \tag{4.36}$$

$$Z_2 = X_2 \oplus Y_{22} \oplus Y_{12} = X_2 \oplus \bar{Y}_2 \tag{4.37}$$

To analyze the power of the attack $P_a$ we wish to determine the resulting probability mass functions for $\bar{Y}_1$ and $\bar{Y}_2$ in Eqs. (4.36) and (4.37). We proceed by writing $\bar{Y}_1$ in terms of the probabilities of the underlying events as shown in Eq. (4.38) to (4.41). The final probability mass function is given by Eqs. (4.42) and (4.43).

$$\begin{aligned} Pr\{\bar{Y}_1 = 1\} = Pr\{&(a \quad \text{and} \quad \tilde{c}) \quad \text{or} \quad (a \quad \text{and} \quad \tilde{d}) \\ &\text{or} \quad (b \quad \text{and} \quad \tilde{c}) \quad \text{or} \quad (b \quad \text{and} \quad \tilde{d}) \\ &\text{or} \quad (c \quad \text{and} \quad \tilde{a}) \quad \text{or} \quad (c \quad \text{and} \quad \tilde{b}) \\ &\text{or} \quad (d \quad \text{and} \quad \tilde{a}) \quad \text{or} \quad (d \quad \text{and} \quad \tilde{b})\} \end{aligned} \tag{4.38}$$

$$\begin{aligned} Pr\{\bar{Y}_1 = 1\} = Pr\{&(a \quad \text{and} \quad (\tilde{c} \quad \text{or} \quad \tilde{d})) \\ &\text{or} \quad (b \quad \text{and} \quad (\tilde{c} \quad \text{or} \quad \tilde{d})) \\ &\text{or} \quad (c \quad \text{and} \quad (\tilde{a} \quad \text{or} \quad \tilde{b})) \\ &\text{or} \quad (d \quad \text{and} \quad (\tilde{a} \quad \text{or} \quad \tilde{b})) \end{aligned} \tag{4.39}$$

$$Pr\{\bar{Y}_1 = 1\} = Pr\{(a \cup b) \cap (\tilde{c} \cup \tilde{d})\} + Pr\{(c \cup d) \cap (\tilde{a} \cup \tilde{b})\} \tag{4.40}$$

$$Pr\{\bar{Y}_1 = 1\} = Pr\{a \cup b\} \cdot Pr\{\tilde{c} \cup \tilde{d}\} + Pr\{c \cup d\} \cdot Pr\{\tilde{a} \cup \tilde{b}\} \tag{4.41}$$

$$Pr\{\bar{Y}_1 = 1\} \triangleq Q_1 = (q_1 + q_2) \cdot (\tilde{q}_3 + \tilde{q}_4) + (q_3 + q_4) \cdot (\tilde{q}_1 + \tilde{q}_2) \tag{4.42}$$

$$\bar{Y}_1 = \begin{cases} 1 \quad \text{w.p} \quad Q_1 \\ \\ 0 \quad \text{w.p} \quad 1 - Q_1 \end{cases} \tag{4.43}$$

A similar analysis may be performed to obtain the probability mass function for $\bar{Y}_2$ which we show here in its entirety for completeness:

$$\begin{aligned} Pr\{\bar{Y}_2 = 1\} = Pr\{&(a \quad \text{and} \quad \tilde{b}) \quad \text{or} \quad (a \quad \text{and} \quad \tilde{d}) \\ &\text{or} \quad (b \quad \text{and} \quad \tilde{a}) \quad \text{or} \quad (b \quad \text{and} \quad \tilde{c}) \\ &\text{or} \quad (c \quad \text{and} \quad \tilde{b}) \quad \text{or} \quad (c \quad \text{and} \quad \tilde{d}) \\ &\text{or} \quad (d \quad \text{and} \quad \tilde{a}) \quad \text{or} \quad (d \quad \text{and} \quad \tilde{c})\} \end{aligned} \tag{4.44}$$

$$\begin{aligned} Pr\{\bar{Y}_2 = 1\} = Pr\{&(a \quad \text{and} \quad (\tilde{b} \quad \text{or} \quad \tilde{d})) \\ &\text{or} \quad (b \quad \text{and} \quad (\tilde{a} \quad \text{or} \quad \tilde{c})) \\ &\text{or} \quad (c \quad \text{and} \quad (\tilde{b} \quad \text{or} \quad \tilde{d})) \\ &\text{or} \quad (d \quad \text{and} \quad (\tilde{a} \quad \text{or} \quad \tilde{c})) \end{aligned} \tag{4.45}$$

$$Pr\{\bar{Y}_2 = 1\} = Pr\{(a \cup c) \cap (\tilde{b} \cup \tilde{d})\} + Pr\{(b \cup d) \cap (\tilde{a} \cup \tilde{c})\} \tag{4.46}$$

$$Pr\{\bar{Y}_2 = 1\} = Pr\{a \cup c\} \cdot Pr\{\tilde{b} \cup \tilde{d}\} + Pr\{b \cup d\} \cdot Pr\{\tilde{a} \cup \tilde{c}\} \tag{4.47}$$

$$Pr\{\bar{Y}_2 = 1\} \triangleq Q_2 = (q_1 + q_3) \cdot (\tilde{q}_2 + \tilde{q}_4) + (q_2 + q_4) \cdot (\tilde{q}_1 + \tilde{q}_3) \tag{4.48}$$

$$\bar{Y}_2 = \begin{cases} 1 \quad \text{w.p} \quad Q_2 \\ \\ 0 \quad \text{w.p} \quad 1 - Q_2 \end{cases} \tag{4.49}$$

The power of the cross stealthy attack based on these results is thus given by

Table III. Comparison of the Expected Power of Attack $E[P_a]$ for Strategy Types

| Strategy Type | Strategy | $E[P_a]$ |
|---|---|---|
| pure | $q_1 = 1$ | 0 |
| doublet | $q_1 = q_2 = 1/2$ | 1/3 |
| triplet | $q_1 = q_2 = q_3 = 1/3$ | 2/5 |
| quadruplet | $q_1 = q_2 = q_3 = q_4 = 1/4$ | 1/2 |

Eqs. (4.50) and (4.51) where $P_a(l_i)$ denotes the power of the attack by the hostile network upon legitimate node $l_i$.

$$P_a(l_1) = Q_1 \tag{4.50}$$

$$P_a(l_2) = Q_2 \tag{4.51}$$

Based on Eqs. (4.50) and (4.51) and the list of all pure, doublet, triplet and quadruplet equilibria as given in proposition 2, the average expected power of the attack $E[P_a]$ for each strategy type can be determined. The results are shown in Table III where we observe that unlike in the case of the stealth $\mathcal{S}_c$, the average power of the attack increases with an increase in the mixing that the hostile nodes perform. Thus by increasing the level of mixing, the hostile nodes are decreasing their stealth while simultaneously increasing the power of the attack. It is thus not clear a priori which alternative produces the better overall result for the hostile network.

To investigate this trade-off between the level of stealth $\mathcal{S}_c$ and the power of the attack $P_a$, we employ the joint power-communication-detection $PCD$ metric shown in Eq. (4.52). We note that in the stealthy cross attack the hostile nodes do not explicitly communicate with each other and hence the number of communications utilized is zero. We also note that the probability of attack detection $P_D$ is related

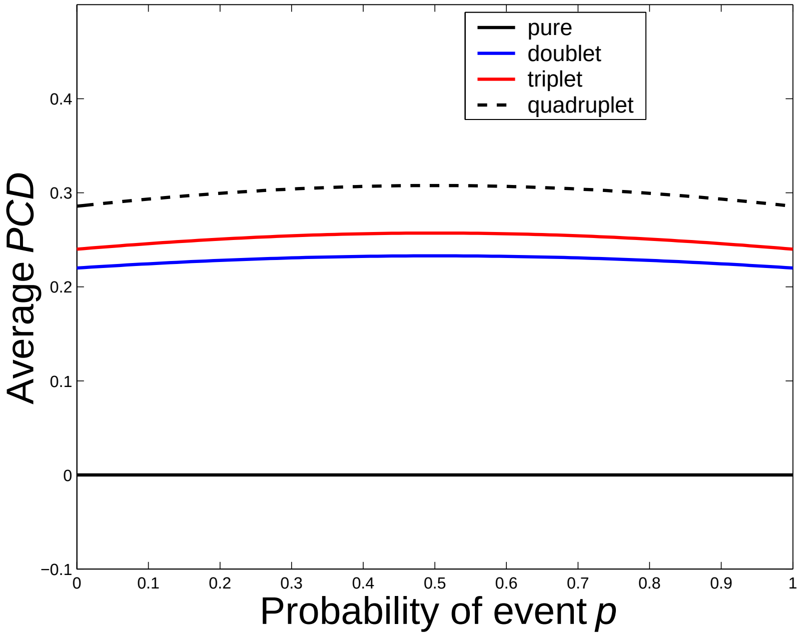


Fig. 31. Comparison of the average power-communication-detection $PCD$ metric for various strategy types over the range of probability $p$ of an event for the cross attack.

to the stealth condition $\mathcal{S}_c$ via the relationship $P_D = 1 - \mathcal{S}_c$ where we recall that the stealth condition is a *relative* measure of avoiding detection. We thus obtain the $PCD$ as experienced by legitimate sensors $l_1$ and $l_2$ as given in Eqs. (4.53) and (4.54).

$$PCD = \frac{\text{No. attacked nodes}}{(1 + \text{No. communications}) \cdot (1 + P_D)} \tag{4.52}$$

$$PCD_{L1} = \frac{Q_1}{1 \cdot (1 + P_D)} \tag{4.53}$$

$$PCD_{L2} = \frac{Q_2}{1 \cdot (1 + P_D)} \tag{4.54}$$

The results of the $PCD$ comparison are displayed in Figure 31 where the average power-communication-detection metric is shown over the range of probability $p$ for the various strategy types. As seen in Figure 31, when both the stealth and the power of the attack are taken into account, the quadruplet strategy performs better than all the other strategies over the entire range of probability $p$, followed by the triplets, the doublets and finally the pure strategies. This result is very significant for the hostile network in terms of optimal attack selection. As noted in proposition 2, the equilibria for both the pure actions case and the mixed actions case are not unique. However when the overall performance is considered via the $PCD$ metric, the optimal choice is that of a quadruplet. This is significant since there exists only one quadruplet equilibrium, namely the $(\mathbf{q}, \tilde{\mathbf{q}})$ equilibrium where $\mathbf{q} = [1/4, 1/4, 1/4, 1/4]$ and where $\tilde{\mathbf{q}} = [1/4, 1/4, 1/4, 1/4]$. Thus there exists a unique optimal solution that each hostile node $h_i$ can implement to achieve the optimal stealth and power of attack trade-off. This result is summarized in remark 4.

**Remark 4** *For the stealthy cross attack game, the unique optimal action of each hostile node $h_i$ is to attack according to the quadruplet mix given by $\mathbf{q} = [1/4, 1/4, 1/4, 1/4]$ for $h_1$ and by $\tilde{\mathbf{q}} = [1/4, 1/4, 1/4, 1/4]$ for $h_2$ in order to achieve the best stealth $\mathcal{S}_c$ and power of attack $P_a$ trade-off.*

## 3. Attack Implications

Analysis of the stealthy cross attack demonstrates that there exist multiple pure and mixed strategy Nash equilibria for the hostile network and that these equilibria achieve different levels of performance in terms of the stealth $\mathcal{S}_c$, in terms of the power of attack $P_a$ and in terms of the joint power-communication-detection $PCD$ metric. Based on its deployment and goals, the hostile network may thus generate a strategy priority list for the equilibria that it wishes to implement in order to achieve a desired performance based on a given metric. To achieve the optimal $PCD$ performance for instance, the hostile network prefers to implement the following equilibria listed in order of decreasing $PCD$ performance and thus decreasing attack preference: $1-$ the unique quadruplet equilibrium, $2-$ a triplet equilibrium, $3-$ a doublet equilibrium and $4-$ a pure equilibrium. Importantly, the order of the preference list changes depending on the performance metric of interest.

In this section we wish to consider the coordination ramifications of a strategy preference list (such as the PCD preference list) for hostile nodes that are deployed in an environment for the purposes of a stealthy cross attack where each hostile node makes decisions that are independent of the other hostile node. To facilitate the exposition, we discuss the ramifications with respect to a 2D grid-based world and discuss the implications for general deployments. Specifically, we initially interpret the 2D world as being comprised of a grid where nodes (hostile or legitimate) are placed at the nodes of the grid and where mobility occurs along the edges of the grid. A sample scenario is illustrated in Figure 32 where two hostile nodes $h_1$ and $h_2$ (marked by squares) are deployed in the vicinity of two legitimate nodes $l_1$ and $l_2$ (marked by circles). In this context, the goal of the hostile nodes is to achieve a stealthy cross attack at the next time step irrespective of the current configuration (the current configuration of the four nodes may not be an equilibrium point for the hostile network in terms of attack stealth or attack $PCD$). To simplify the exposition we employ the following definitions and assumptions.

1. The actuation radius $a.r$ of each hostile node $h_i$ is normalized to $a.r = 1$.

2. The sensing radius $s.r$ of each legitimate sensor $l_i$ is normalized to $s.r = 1$.

3. Each edge of a grid joining two node points is of normalized grid length $g.l = 1$.

4. Within a single time step, each hostile node $h_i$ traverses a distance equal to one

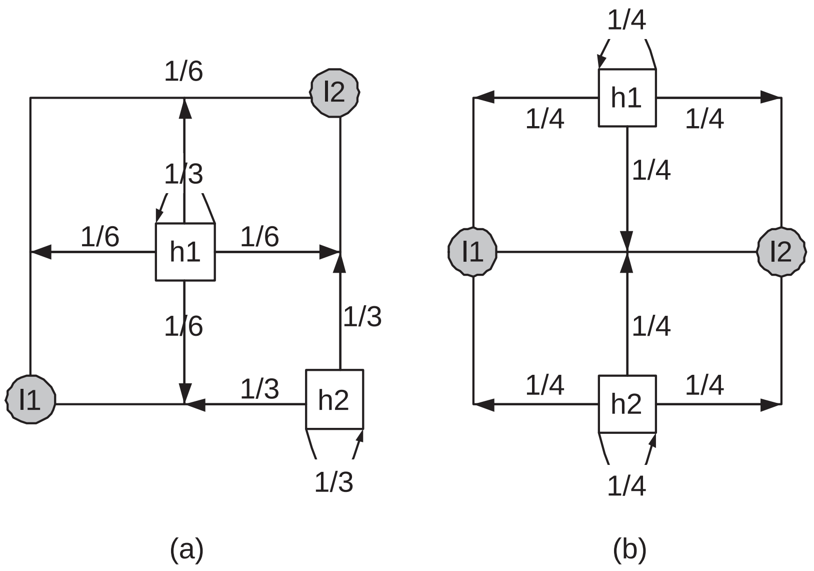


Fig. 32. (a) Implementation of triplet $(a, b, c)$ and $(\tilde{a}, \tilde{b}, \tilde{c})$. (b) Implementation of quadruplet $(a, b, c, d)$ and $(\tilde{a}, \tilde{b}, \tilde{c}, \tilde{d})$.

grid length, that is, a grid distance of $g.l = 1$.

These simplifying assumptions can be understood in relation to the scenarios depicted in Figures 32a and 32b. In both Figures 32a and 32b, neither of the hostile nodes $h_1$ or $h_2$ is currently in a location from which it can perpetrate an attack on either of $l_1$ or $l_2$ based on the assumption that $a.r = 1$ and $s.r = 1$. Thus if none of the hostile or legitimate nodes move, the hostile nodes are effectively in a position to implement attack strategy $a$ and $\tilde{a}$ from Eq. (4.9), that is, $\mathbf{q} = [1, 0, 0, 0]$ and $\tilde{\mathbf{q}} = [1, 0, 0, 0]$. For the general case of legitimate and hostile node deployment in the 2D grid world, the hostile nodes require a mechanism for implementing the attack equilibria on the priority list. We wish to investigate the implications stemming from this need in terms of the required coordination among the hostile nodes.

**Example 3** *This example illustrates the representative coordination approach that*

Table IV. Output of Algorithm 4 for Example 3

| **Direction** | $\mathbf{h_1}$ | $\mathbf{h_2}$ |
|---|---|---|
| up | b | b |
| down | c | none |
| left | b | none |
| right | c | c |
| stay | a | a |

Table V. Output of Algorithm 5 for Example 3

| **Action from Priority List** | $\mathbf{h_1}$ | $\mathbf{h_2}$ |
|---|---|---|
| quadruplet (a,b,c,d) | not possible for $h_1$ or $h_2$ | not possible for $h_2$ or $h_1$ |
| quadruplet (a,b,c,d) | move to next action | move to next action |
| triplet (a,b,c) | possible for $h_1$ and $h_2$ | possible for $h_2$ and $h_1$ |
| triplet (a,b,c) | find prob assignment | find prob assignment |

*may be utilized by the hostile nodes to enact a stealthy cross attack without active communication during the attack. The example corresponds to the scenario depicted in Figure 32a. Tables IV and V correspond to the outputs of Algorithms 4 and 5.*

Table VI. Output of Algorithm 6 for Example 3

| $\mathbf{h_1}$ **count** | $\mathbf{h_1}$ **prob** | $\mathbf{h_2}$ **count** | $\mathbf{h_2}$ **prob** |
|---|---|---|---|
| $count(a) = 1$ | (stay), $w.p$ 1/3 | $count(a) = 1$ | (stay) $w.p$ 1/3 |
| $count(b) = 2$ | (up, right), $w.p$ 1/6 each | $count(b) = 1$ | (up) $w.p$ 1/3 |
| $count(c) = 2$ | (down, left), $w.p$ 1/6 each | $count(c) = 1$ | (left) $w.p$ 1/3 |

Table VII. Sample Priority List for $PCD$ Metric

| **Preferred Category** | **Preferred Action** |
|---|---|
| quadruplet | (a,b,c,d) |
| triplet | (a,b,c), (a,b,d), (a,c,d), (b,c,d) |
| doublet | (a,d), (b,c), (a,b), (a,c), (b,d), (c,d) |
| pure | (a), (b), (c), (d) |

To illustrate the key coordination issues for the hostile network H, we consider a representative attack methodology for each hostile node $h_i$ which is summarized in Algorithms 4, 6 and 5 and through Example 3 which explores the scenario of Figure 32a in terms of Algorithms 4, 6 and 5. In Algorithm 4, each hostile node $h_i$ associates each direction of travel (up, down, left, right and stay at its current location) with a resulting strategy. For instance in Figure 32a, traveling to the left enables hostile node $h_1$ to attack legitimate sensor $l_1$ but not legitimate sensor $l_2$, thus enacting attack strategy $c$ where $\mathbf{q} = [0, 0, 1, 0]$. Importantly we note that use of Algorithm 4 allows a hostile node $h_i$ to determine its *own* possible attack actions and that it requires knowledge of the positions of the legitimate sensors $l_1$ and $l_2$. We observe that to carry out an attack without explicit inter-node communication, each hostile node $h_i$ must also know the position of the other hostile node $h_j$. Such position knowledge allows the determination of the strategy set of the *other* hostile node by re-running Algorithm 4 based on the location of the other hostile node. Thus after running Algorithm 4, each hostile node possesses a list of associations between each direction of movement and the resulting attack strategy for both $h_1$ and $h_2$ as shown in Table V in Example 3.

Algorithm 4 should thus be applied by each hostile node to find its own actions as well as the actions of the other hostile node and this procedure requires information regarding the position of all four nodes. To plan an attack without explicit communications, Algorithm 5 is applied by each hostile node following Algorithm 4. Algorithm 5 enables each node to identify which of the equilibria from the priority list can be implemented by *both* hostile nodes. This is illustrated in Table V as the algorithm pertains to Example 3. Finally, each node runs Algorithm 6 to assign a probability of moving in each of the five directions (up, down, left, right, stay). Importantly, this assignment of probabilities implements the desired equilibrium as shown in Table VI and Figure 32a. For the case of Example 3 of Figure 32a, the hostile nodes are not both able to implement the quadruplet that is at the top of their priority list from Table VII. They are both able to implement the second equilibrium from the priority list, namely the triplet $a, b, c$ and $\tilde{a}, \tilde{b}, \tilde{c}$. Based on the analysis and results from proposition 2, a mixed Nash equilibrium requires that each hostile node $h_i$ mixes with equal probability of 1/3 among actions $a$, $b$ and $c$ in order to implement this triplet. Based on their current locations, each hostile node must thus move with the probabilities prescribed in Table VI and Figure 32a. For comparison, Figure 32b depicts a sample scenario and an assignment of probabilities that enable H to implement the quadruplet.

We now summarize the implications for hostile node coordination for the case of a cross stealthy attack. First we conclude that it is indeed possible in principle for the hostile nodes to achieve a stealthy cross attack without explicit inter-node communication. Such an attack can be achieved through node cooperation as illustrated through the example Algorithms 4, 5 and 6. We note two important requirements to achieve the attack under this scenario. First, each hostile node must know the position of all the other nodes in the vicinity that either participate in the attack or are affected by the attack (in this case the two legitimate nodes and the other hostile node). Although we have assumed a grid-like world in the example, this position-knowledge requirement also applies to non-grid models. Indeed this information is required in order for each hostile node to compute its next position based on the positions of the other nodes and based on the attack radius and sensing radius models (assumed here to be normalized to 1). The second observation is that to avoid communication, the hostile nodes must share the same priority list (such as pre-loaded in memory). Together with the location information, the priority list enables each hostile node to determine which attack is implementable and which attack will actually be carried out based on the priority. We thus conclude that stealthy cross attacks that do not require active inter-node communications are possible but that they require knowledge of all node positions and the possession of priority lists.

**Algorithm 4** Find Possible Actions for Hostile Node $h_i$

**Require:** Input.

$h_i$ knows the location of all other nodes including itself.

{List of Possible Directions: Dir = [up, down, left, right, stay]. Indexed by $k$.}

{List of Possible Actions: Act = [a, b, c, d, empty]. Indexed by $m$.}

**Ensure:** This algorithm associates each possible direction $Dir(k)$ with the action $Act(m)$ resulting from that direction.

```
for Each member of the list Dir do
    Compute new location of $H_i$
    if No overlap with $L_1$ and $L_2$ and not outside world then
        Classify action at new location
        if Affect $L_1$ and $L_2$ then
            Assign Dir(k)= Act(4) (action d)
        else if Affect not $L_1$ and $L_2$ then
            Assign Dir(k) = Act(3) (action c)
        else if Affect $L_1$ and not $L_2$ then
            Assign Dir(k) = Act(2) (action b)
        else
            Assign Dir(k) = Act(1) (action a)
        end if
    else
        Direction results in overlap or outside world: Dir(k) = 5 (empty)
    end if
end for
```

**Algorithm 5** Find Implementable Cross Stealthy Equilibrium for H

```
Require: Input:
    1 - Strategy to implement (from Strategy Priority List)
    2 - Direction-Action association list for $h_1$ and $h_2$ (Output of Algorithm 4).
Ensure: Achieve a deployment for H at the next time step that implements a stealthy
    cross attack on L based on the Priority List without inter-node communication.
for each action $k$ in the priority list do
    if $h_1$ and $h_2$ can both implement action $k$ then
        Find assignment of probabilities for each direction of travel to implement
        action $k$ by running Algorithm 6. Deployment is complete.
    else
        Move to the next item $k + 1$ in the priority list
    end if
end for
```

**Algorithm 6** Assign Probabilities to Actions of $h_i$

```
Require: Input:
    1- Implementable action for H (output of Algorithm 5)
    2- Direction-Action association list for $h_1$ and $h_2$ (output of Algorithm 4).
Ensure: This algorithm assigns a probability of moving to each of the possible directions Dir = [up, down, left, right, stay] such that an equilibrium is achieved.
For the equilibrium to be implemented (output of Algorithm 5):
for all non-empty directions in the list Dir do
    Count number of directions that correspond to each Action $j$
    if $Dir(k) ==$ Action$j$ then
        $count_j = count_j + 1$
    end if
end for
$ProbDir_k = 1/($No. Actions $\cdot count_j)$ {Each action is assigned equal probability to achieve equilibrium and all directions that implement each action are assigned equal probability.}
```

## D. Secure Data Acquisition Results

In this section we investigate defense strategies for the legitimate sensor network L for the case of a stealthy cross attack by the hostile network H. As modeled in Section B, the cluster head receives decisions regarding an event from legitimate sensors that may be attacked by hostile nodes deployed in the area. We show how game theoretic analysis of the optimal attack and defense strategies from Section C enables the use of established detection techniques to uncover the attack at the cluster head and to mitigate the attack at the legitimate sensors.

### 1. Defense Analysis

Based on the model of Section B for the stealthy cross attack, the cluster head receives decisions $z_1$ and $z_2$ regarding an event of interest in the environment from legitimate sensors $l_1$ and $l_2$ where the random variables $Z_1$ and $Z_2$ are given in Eqs. (4.55) and (4.56).

$$Z_1 = X_1 \oplus Y_{11} \oplus Y_{21} = X_1 \oplus \bar{Y}_1 \tag{4.55}$$

$$Z_2 = X_2 \oplus Y_{22} \oplus Y_{12} = X_2 \oplus \bar{Y}_2 \tag{4.56}$$

In Section C the probability mass functions for $\bar{Y}_1$ and $\bar{Y}_2$ were determined as summarized in Eqs. (4.57) through (4.60).

$$\bar{Y}_1 = \begin{cases} 1 & \text{w.p} \quad Q_1 \\ 0 & \text{w.p} \quad 1 - Q_1 \end{cases} \tag{4.57}$$

$$Q_1 = (q_1 + q_2) \cdot (\tilde{q}_3 + \tilde{q}_4) + (q_3 + q_4) \cdot (\tilde{q}_1 + \tilde{q}_2) \tag{4.58}$$

$$\bar{Y}_2 = \begin{cases} 1 & \text{w.p} \quad Q_2 \\ 0 & \text{w.p} \quad 1 - Q_2 \end{cases} \tag{4.59}$$

$$Q_2 = (q_1 + q_3) \cdot (\tilde{q}_2 + \tilde{q}_4) + (q_2 + q_4) \cdot (\tilde{q}_1 + \tilde{q}_3) \tag{4.60}$$

The cluster head thus receives a realization of the decision vector $\mathbf{z} = [z_1 z_2]$ and based on this information attempts to decide whether or not an attack has occurred. The cluster head thus wishes to distinguish between hypothesis $\mathcal{H}_0$ and hypothesis $\mathcal{H}_1$ given in Eqs. (4.61), (4.62) and (4.63).

$$\mathcal{H}_0 \quad : \quad \text{normal operation}, \mathbf{Z_i} \sim Bern(p) \tag{4.61}$$

$$\mathcal{H}_1 \quad : \quad \text{attacked operation}, \mathbf{Z_i} \sim Bern(r_i) \tag{4.62}$$

$$r_i = p + Q_i - 2p \cdot Q_i \quad \text{for} \quad i \in [1, 2] \tag{4.63}$$

The optimal detector to distinguish between these two hypotheses based on the Neyman-Pearson (NP) paradigm utilizes the likelihood ratio $\Lambda(z_1 z_2)$ given in Eq. (4.64) where $p$ is the probability of an event and $f(z_1, z_2)$ is the probability mass function of $z_1$ and $z_2$ given in Eqs. (4.65) and (4.66). The threshold $\mathcal{T}$ in Eq. (4.64) is chosen based on Eq. (4.67) such that a desired probability of false alarm $P_{FA} = \alpha$ is achieved. Based on the chosen $\alpha$ in the NP paradigm, the maximal probability of detection $P_D = \beta$ is obtained via Eq. (4.68).

$$\Lambda(z_1 z_2) = \frac{f(z_1, z_2)}{p^{z_1 + z_2}(1-p)^{2 - z_1 - z_2}} \underset{\mathcal{H}_0}{\overset{\mathcal{H}_1}{\gtrless}} \mathcal{T} \tag{4.64}$$

$$f(z_1, z_2) = \begin{cases} r_1 r_2 & z_1 = 1 \quad z_2 = 1 \\ r_1(1 - r_2) & z_1 = 1 \quad z_2 = 0 \\ (1 - r_1) r_2 & z_1 = 0 \quad z_2 = 1 \\ (1 - r_1)(1 - r_2) & z_1 = 0 \quad z_2 = 0 \end{cases} \tag{4.65}$$

$$\begin{aligned} f(z_1, z_2) = r_1 r_2 \cdot \mathbb{I}_{z_1=1}\mathbb{I}_{z_2=1} + r_1(1 - r_2) \cdot \mathbb{I}_{z_1=1}\mathbb{I}_{z_2=0} + \\ (1 - r_1) r_2 \cdot \mathbb{I}_{z_1=0}\mathbb{I}_{z_2=1} + (1 - r_1)(1 - r_2)\mathbb{I}_{z_1=0}\mathbb{I}_{z_2=0} + \end{aligned} \tag{4.66}$$

$$\begin{aligned} \alpha &= Pr\{\Lambda(z_1 z_2) > \mathcal{T} | p^{z_1+z_2}(1 - p)^{2-z_1-z_2}\} \\ &= \sum_{z_1 z_2 : \Lambda(z_1 z_2) > T} p^{z_1+z_2}(1 - p)^{2-z_1-z_2} \end{aligned} \tag{4.67}$$

$$\begin{aligned} \beta &= Pr\{\Lambda(z_1 z_2) > \mathcal{T} | f(z_1, z_2)\} \\ &= \sum_{z_1 z_2 : \Lambda(z_1 z_2) > T} f(z_1, z_2) \end{aligned} \tag{4.68}$$

Though optimal with respect to the NP paradigm, the detector of Eq. (4.64) is not truly implementable for the legitimate network L without game theoretic analysis of the opponent H due to missing information. Specifically, the detection statistic $\Lambda(z_1 z_2)$ requires knowledge of the parameters $r_1$ and $r_2$ which in turn depend on knowledge of $Q_1$ and $Q_2$ from Eqs. (4.58) and (4.60). Since $Q_1$ and $Q_2$ depend on the attack actions $\mathbf{q}$ and $\tilde{\mathbf{q}}$ of hostile nodes $h_1$ and $h_2$, they are generally unknown without analysis. We also note that in certain applications, the cluster head may not be able to distinguish among the two legitimate sensors $l_1$ and $l_2$. That is, the cluster head may simply be aware of the total weight $w \in \{0, 1, 2\}$ received from both sensors but not distinguish which sensor sent which decision and thus not have access to $z_1$ and $z_2$ itself but rather have access to an overall weight $w$.

Motivated by these considerations, we examine a sub-optimal version of the Neyman-Pearson detector which relies on the overall weight $w$ instead of the individual sensor decisions $z_1$ and $z_2$. We note that the transition from the use of the detailed $z_1$ and $z_2$ information to the aggregate weight $w$ information constitutes a loss of information and results in a sub-optimal version of the NP detector. The sub-optimal NP detector is given by Eq. (4.69) and is based on the detection statistic $\Lambda(w)$ where the probability mass function $f(w)$ is given in Eqs. (4.70) and (4.71). The threshold $\mathcal{T}$ in Eq. (4.69) is set based on a desired probability of false alarm $\alpha$ from Eq. (4.72) and the resulting probability of detection is given by Eq. (4.73).

$$\Lambda(w) = \frac{f(w)}{\binom{2}{w} p^w (1-p)^{2-w}} \overset{\mathcal{H}_1}{\underset{\mathcal{H}_0}{\gtrless}} \mathcal{T} \tag{4.69}$$

$$f(w) = \begin{cases} r_1 r_2 & w = 2 \\ r_1(1-r_2) & w = 1 \\ (1-r_1)r_2 & w = 1 \\ (1-r_1)(1-r_2) & w = 0 \end{cases} \tag{4.70}$$

$$\begin{aligned} f(w) = {} & r_1 r_2 \cdot \mathbb{I}_{w=2} + r_1(1-r_2) \cdot \mathbb{I}_{w=1} + \\ & (1-r_1)r_2 \cdot \mathbb{I}_{w=1} + (1-r_1)(1-r_2)\mathbb{I}_{w=0} \end{aligned} \tag{4.71}$$

$$\begin{aligned} \alpha &= Pr\{\Lambda(w) > \mathcal{T} \quad | \quad \binom{2}{w} p^w (1-p)^{2-w}\} \\ &= \sum_{w:\Lambda(w)>\mathcal{T}} \binom{2}{w} p^w (1-p)^{2-w} \end{aligned} \tag{4.72}$$

$$\begin{aligned} \beta &= Pr\{\Lambda(w) > \mathcal{T} | f(w)\} \\ &= \sum_{\substack{w=0 \\ w:\Lambda(w)>\mathcal{T}}}^{2} f(w) \end{aligned} \tag{4.73}$$

We make a key observation regarding the sub-optimal detector of Eq. (4.69). Although the detection statistic $\Lambda(w)$ no longer requires knowledge of the individual $z_1$ and $z_2$ sensor decisions, the underlying probability mass function $f(w)$ still depends on parameters $r_1$ and $r_2$ and thus on the attackers' actions $\mathbf{q}$ and $\tilde{\mathbf{q}}$. Thus analysis of the attackers' optimal attack strategies is required for attack detection. This is in contrast with the case of the stealthy direct attack. In the stealthy direct attack, simplification of the NP detector eliminates the need for the attack parameters though importantly, the attack parameters are still required in order to determine the detector's $P_{FA}$-$P_D$ performance. Thus we conclude that in the case of the stealthy cross attack, the legitimate network L faces a more challenging detection scenario.

In the analysis of Section C, we showed that multiple optimal pure and mixed equilibria exist for the hostile network H under the stealth $\mathcal{S}_c$ metric. However we showed that the optimal attack strategies to maximize $\mathcal{S}_c$ are restricted to the doublet class of mixed equilibria. Furthermore we showed that when the overall power-communication-detection $PCD$ metric is considered, there exists a unique optimal equilibrium for the attacker, namely the unique quadruplet equilibrium where $\mathbf{q} = [1/4, 1/4, 1/4/, 1/4]$ and where $\tilde{\mathbf{q}} = [1/4, 1/4, 1/4/, 1/4]$. Such analysis thus enables the legitimate network to predict the actions of the hostile network and to utilize both the optimal and sub-optimal Neyman-Pearson detectors of Eqs. 4.64 and 4.69 for attack detection. Furthermore, based on the results of Section C, in order to perform attack mitigation at the individual sensors, the legitimate network should select a local sensor threshold $T_h$ that yields either a small or large probability $p$ of an event. This result is thus consistent with the mitigation strategies obtained for the case of the stealthy direct attack.

Table VIII. Ordering of Stealth Condition by Strategy Type

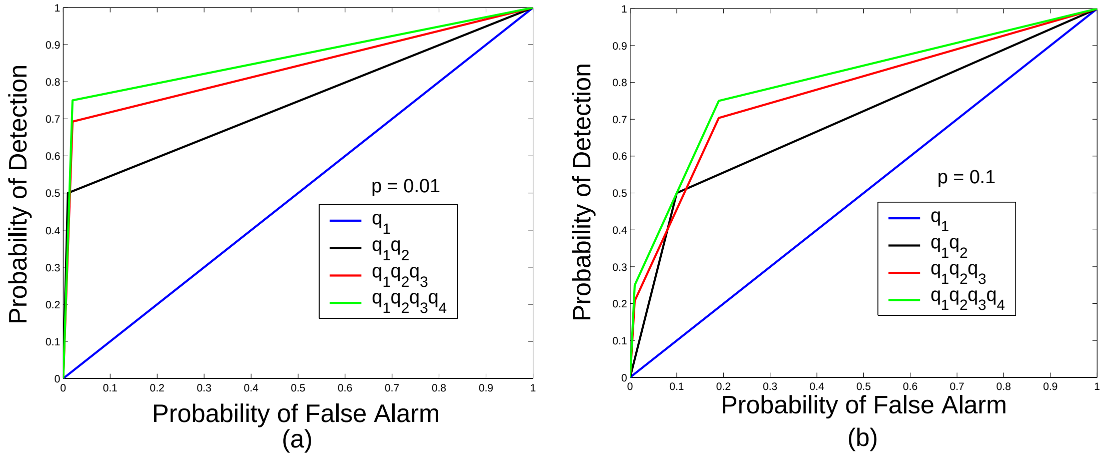
| Strategy Type | Relative Stealth $\mathcal{S}_c$ |
|---|---|
| pure | 1 |
| doublet | $(1/2)(1 + (1/3)\delta_p)$ |
| triplet | $(1/3)(1 + (2/3)\delta_p)$ |
| quadruplet | $(1/4)(1 + \delta_p)$ |

### 2. Defense Performance

In this section we wish to examine the performance of the defense strategies of the legitimate sensor network L in the case of the stealthy cross attack by the hostile network H. We show that the stealth condition $\mathcal{S}_c$ is consistent for both the legitimate and the hostile networks in terms of attack detection at the cluster head. We also show that as in the case of the stealthy direct attack, the legitimate network L may mitigate the stealth of the attack through proper choice of the sensor decision threshold $T_h$.

The analysis and results of Section C indicate that the hostile network H may achieve several pure or mixed attack equilibria that can be classified into different strategy types with varying (relative) levels of stealth $\mathcal{S}_c$. Specifically as discussed in Section C and recapped in Table VIII, the hostile network achieves a higher *relative* level of stealth by implementing the pure equilibrium strategies. Second in terms of achieving a maximal level of stealth are the doublet equilibria followed by the triplet equilibria and finally the quadruplet equilibrium.

To assess the effectiveness of the stealth condition in selecting attack and defense strategies, we wish to investigate the (absolute) stealth of the attack for the various types of equilibria by considering the attack detection performance at the cluster head. Figures 33a and 33b present a comparison of the $P_D$-$P_{FA}$ probability



(a)

(b)

Fig. 33. Comparison of the $P_D$-$P_{FA}$ performance among pure strategies, doublets, triplets and quadruplets for (a) $p = 0.01$. (b) $p = 0.1$.

of detection and false alarm performance between pure strategies, doublets, triplets and quadruplets for the case of $p = 0.01$ and $p = 0.1$ respectively. As seen in these figures, the performance of the optimal detector does indeed follow the predictions of the stealth condition. That is, mixing with a quadruplet strategy produces a $P_D$-$P_{FA}$ performance which is best for detecting the attack and worst for maintaining stealth as predicted by the stealth condition for both networks. Mixing among triplets produces a better $P_D$-$P_{FA}$ performance than mixing among doublets. Mixing among doublets in turn produces a better $P_D$-$P_{FA}$ performance than playing with a pure strategy. As in Section C we note however that playing with a pure strategy results in a power of attack $P_a = 0$ and is thus undesirable for the hostile network based on those grounds. The $P_D$-$P_{FA}$ performance at the cluster head is thus consistent with the predictions of the stealth condition $\mathcal{S}_c$ for both networks. These results thus also indicate that the best strategy for the hostile network in terms of maximizing stealth is the worst strategy for the legitimate network for attack detection and vice versa.

Similar detection results are displayed in Figures 34a and 34b where the $P_D$-$P_{FA}$ performance among strategies is displayed for the case of $p = 0.3$ and $p = 0.4$.

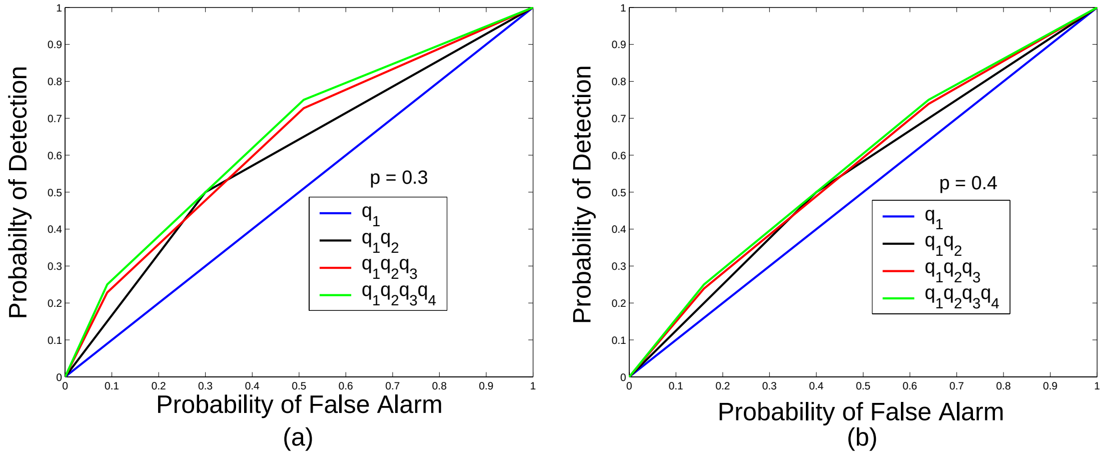
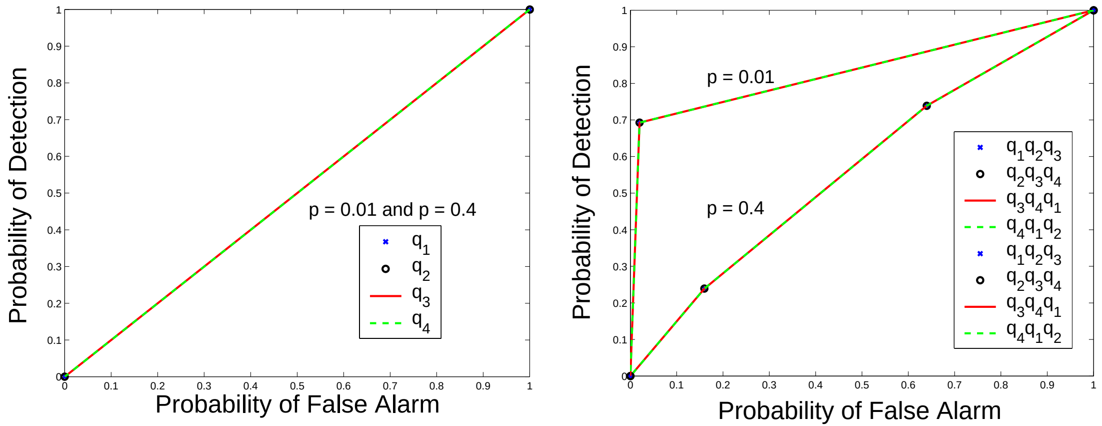


Fig. 34. Comparison of the $P_D$-$P_{FA}$ performance among pure strategies, doublets, triplets and quadruplets for (a) $p = 0.03$. (b) $p = 0.4$.

We make two salient observations regarding these results. First we note that the relative relationship among the various strategy types is preserved over the entire range of probability $p$ of an event. This is important since this relative relationship is predicted by the stealth condition $\mathcal{S}_c$ as shown in the results of Figure 30b and Table VIII. The second important observation stems from a comparison of the $P_D$-$P_{FA}$ curves in Figures 33a, 33b, 34a and 34b. We note that as the value of probability $p$ of an event increases from $p \approx 0$ to $p \approx 0.5$, the overall $P_D$-$P_{FA}$ performance at the cluster head decreases. This is consistent with the prediction of the stealth condition from Section C and Table VIII. It is also consistent with the results obtained for the case of the stealthy direct attack. Importantly we note that due to the symmetry of the stealth condition with respect to $p$, we show the results corresponding to the $[0, 0.5]$ interval with the same results for $1 - p$ corresponding to the $[0.5, 1]$ interval.

We also wish to examine the $P_D$-$P_{FA}$ performance of the attack for different equilibria that fall within the *same* strategy type. Figure 35a depicts the $P_D$-$P_{FA}$ performance of the four possible pure strategies for both the case of $p = 0.01$ and the case of $p = 0.4$. As can be seen from the figure, all pure strategy equilibria result



(a) (b)

Fig. 35. Comparison of the $P_D$-$P_{FA}$ performance for $p = 0.01$ and $p = 0.4$ for (a) different pure strategies. (b) different triplets strategies.

in the same $P_D$-$P_{FA}$ performance at the cluster head and furthermore achieve the same performance irrespective of the probability $p$. This result is consistent with the prediction of the stealth condition from proposition 2 and Table VIII where the same relative level of stealth $\mathcal{S}_c$ is assigned to all equilibria within the pure class. Figure 35b also illustrates this scenario for the case of triplets for $p = 0.01$ and $p = 0.4$ indicating that the predictive relationship is maintained. Finally we summarize the stealth condition results for the stealthy cross attack in remark 5.

**Remark 5** *The stealth condition $\mathcal{S}_c$ of Eq. (4.17) is a relative measure of the hostile network's stealth in the cross attack and is a consistent measure for both the legitimate and hostile networks in terms of the probability of detecting the attack such as under the Neyman-Pearson paradigm.*

### 3. Defense Implications

In this section we wish to investigate the implications of the stealthy cross attack for the defending legitimate L network. We show that the performance of the sub-optimal Neyman-Pearson detector follows closely that of the optimal Neyman-Pearson

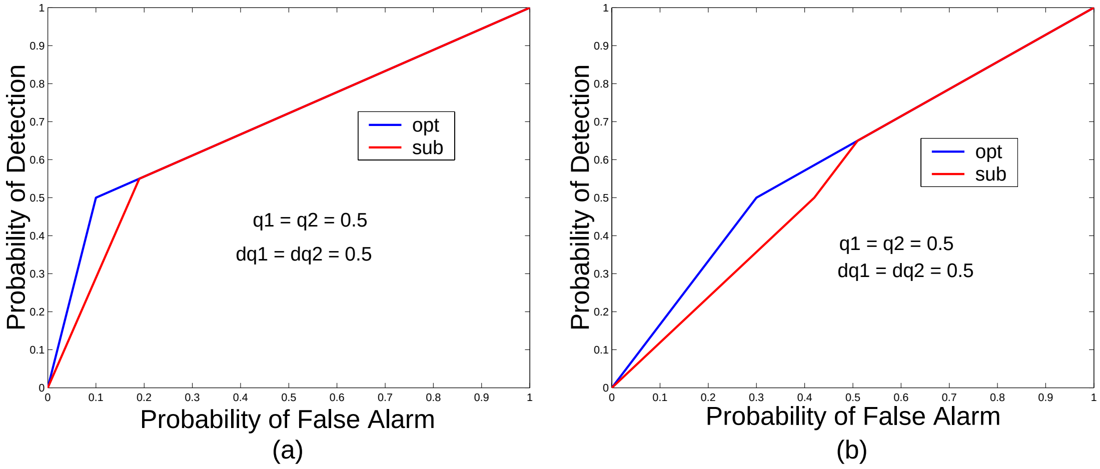


Fig. 36. Optimal vs. sub-optimal detectors for representative doublet mix (a) $p = 0.1$. (b) $p = 0.3$.

detector and that either form of the detector may be utilized based on the needs of the application. The legitimate network thus has at its disposal the necessary tools to detect and mitigate the attack.

As discussed in Section D-1, in certain applications the cluster head of the legitimate network may not be able to distinguish between the individual sensor decisions $z_1$ and $z_2$ but may instead have access to the aggregate weight $w$ of the decision vector $\mathbf{z} = [z_1 z_2]$. In such cases the cluster head may need to utilize a sub-optimal version of the detector as given in Eq. (4.69). Figures 36a and 36b depict the $P_D$-$P_{FA}$ performance of both the optimal and sub-optimal detectors based on the Neyman-Pearson paradigm as given in Eqs. (4.64) and 4.69 for the case of doublet equilibria for probabilities $p = 0.1$ and $p = 0.3$. As can be seen from the comparison, although sub-optimal, the detector based on the aggregate $w$ follows the performance of the optimal detector closely. Figures 36a and 36b depict this comparison for the case of a representative triplet equilibrium and for the case of the unique quadruplet equilibrium for probability $p = 0.3$. As can be seen from these results, the sub-optimal detector achieves the $P_D$-$P_{FA}$ performance of the optimal detector for these cases.

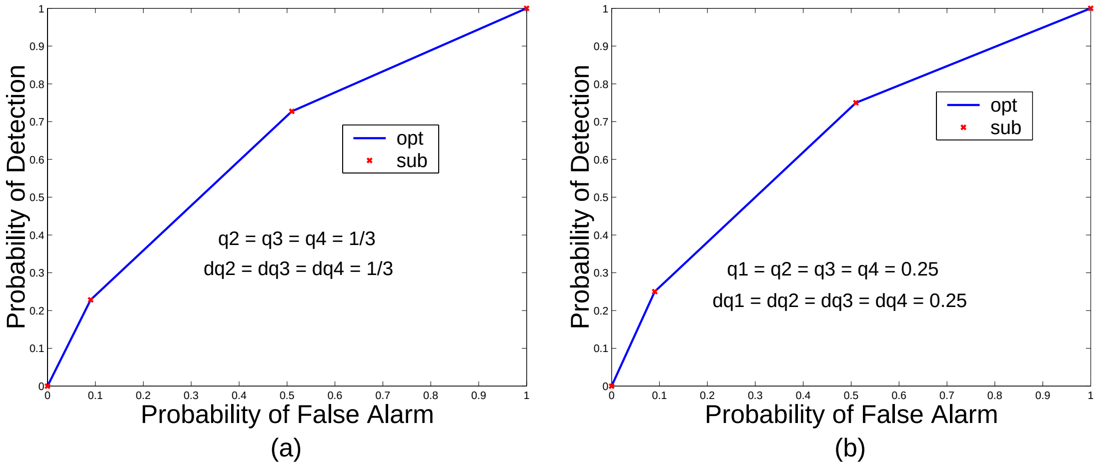


Fig. 37. Optimal vs. sub-optimal detectors for $p = 0.3$ and (a) triplet mix $(b, c, d)$. (b) quadruplet mix $(a, b, c, d)$.

This result is also obtained for different equilibria within the triplet strategy type and within the quadruplet strategy type over the range of probability $p$ as shown in Figures 38a and 38b. Based on these results we make the interesting observation that not only are the doublet equilibria better for the hostile network H in terms of higher (relative and absolute) stealth, they are also better for H in terms of a discrepancy between the optimal and suboptimal detectors. That is, although the sub-optimal detector follows the performance of the optimal detector closely for the doublet equilibria, it occasionally deviates from the optimal performance. This is generally not the case for the triplet and quadruplet equilibria where the sub-optimal detector achieves the performance of the optimal detector.

Based on these results we observe that the optimal defense strategies of the legitimate network for the case of the cross attack parallel the optimal defense strategies obtained for the direct attack. Specifically, it is optimal for the legitimate network L to select the local sensor decision threshold $T_h$ such as to render the probability $p$ of an event small or large. This procedure for L in the case of the stealthy cross attack is summarized in Algorithm 7 which is directly parallel to the defense Algorithm 2

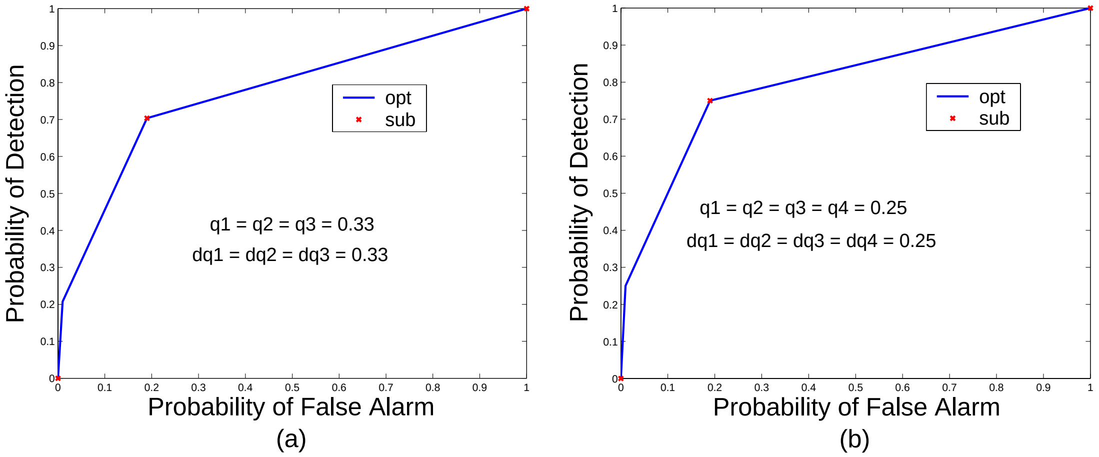


Fig. 38. Optimal vs. sub-optimal detectors for $p = 0.1$ and (a) triplet mix $(a, b, c)$. (b) quadruplet mix $(a, b, c, d)$.

for the case of the direct attack.

## E. Comparisons

In the previous sections we have derived the stealth condition $\mathcal{S}_c$ for the case of the stealthy cross attack. We determined that this condition is consistent for both the legitimate and hostile networks such that it can be utilized to obtain the optimal defense and attack strategies. In this section we wish to compare the stealthy cross attack to the case of the stealthy direct attack where each hostile node attacks only one legitimate sensor directly and we wish to make this comparison for both the case of inter-node communication and no communication. We show interesting properties of these attacks and demonstrate that in terms of the stealth utility $\mathcal{S}_c$, the cross attack achieves a superior level of relative and absolute stealth than the direct attack. We also demonstrate that for the case of a small subset of nodes, the stealthy cross attack without active communication achieves a superior overall power-communication-detection $PCD$ metric compared with the direct attack and

**Algorithm 7** Defense Algorithm for Legitimate Network

```
Ensure: Max attack detection and power of defense given competing hostile network.
Given the probability density function (pdf) of the phenomenon, set the local sensor threshold $T_h$:
if events are expected to be common then
    Set $T_h$ such that $p$ (area under the pdf to the left of $T_h$) is close to 1.
else
    Set $T_h$ such that $p$ is close to 0.
end if
Given information available to the cluster head:
Find optimal attack parameters $\mathbf{q}^*$ and $\tilde{\mathbf{q}}^*$ from Eq. (4.30).
if cluster head receives distinct $z_1$, $z_2$ sensor decisions then
    Utilize detector of Eq. (4.64)
else
    Utilize detector of Eq. (4.69)
end if
```

compared with communication. Next we compare the stealthy cross attack to the case of an uncoordinated attack where each hostile node may select a different attack strategy which does not necessarily result in the optimal stealth equilibrium. These results carry important implications for the design of attack and defense strategies.

### 1. Comparison with Stealthy Direct Attack and Communication

The direct and cross attack models for the hostile network differ in that the cross attack model allows each hostile node to attack more than one legitimate sensor. Conversely as a result of the cross attack, a single legitimate sensor may be attacked by more than one hostile node. Given these two attack models, we wish to determine if allowing cross attacks changes the existing equilibria of the game and if such changes are advantageous or disadvantageous for the hostile network H. Specifically we wish to understand if the cross attack improves the stealth of the attack or causes the attack to be revealed with greater probability.

We begin our comparison with an examination of the stealthy cross attack $\mathcal{G}_c$ and its resulting equilibria. We examine a representative case of a doublet equilibrium via Eq. (4.74) which shows the stealth utility $\mathcal{S}_c$ in terms of a subset of actions of hostile nodes $h_1$ and $h_2$. As shown in Eq. (4.74), we consider the case where hostile node $h_1$ must assign probabilities to its actions $b$ and $c$ while hostile node $h_2$ must assign probabilities to its actions $\tilde{b}$ and $\tilde{c}$. Eqs. (4.75) and (4.76) show the resulting stealth utility for either of the hostile nodes if they choose to match their actions. That is, Eq. (4.75) shows the utility resulting from both hostile nodes choosing matching actions $c$ and $\tilde{c}$ while Eq. (4.76) shows the utility resulting from both hostile nodes choosing matching actions $b$ and $\tilde{b}$. In both cases each hostile node achieves the

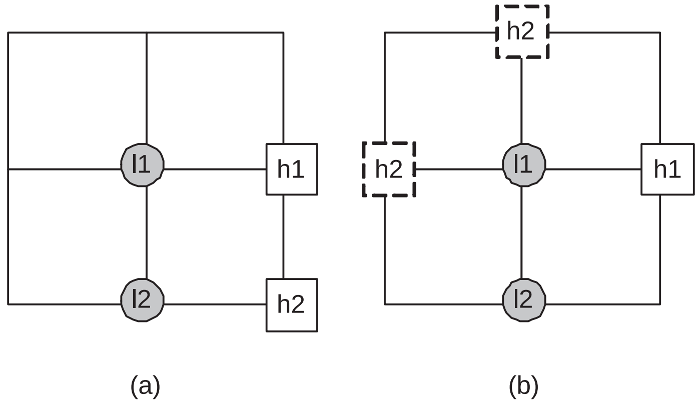


Fig. 39. (a) Cross attack non-equilibrium: $h_1$ plays $c$ and $h_2$ plays $b$. (b) Possible locations of $h_2$ to enact strategy $c$ to match $h_1$'s strategy $c$.

maximal (relative) stealth utility measure of $\mathcal{S}_c = 1$.

$$\mathcal{S}_c = u_2(q_2, q_3, \tilde{q}_2, \tilde{q}_3) = \tilde{q}_2(q_2 + \delta_p q_3) + \tilde{q}_3(q_3 + \delta_p q_2) \tag{4.74}$$

$$\mathcal{S}_c = u_2(q_2 = 1, q_3 = 0, \tilde{q}_2 = 1, \tilde{q}_3 = 0) = 1 \quad \forall p \tag{4.75}$$

$$\mathcal{S}_c = u_2(q_2 = 0, q_3 = 1, \tilde{q}_2 = 0, \tilde{q}_3 = 1) = 1 \quad \forall p \tag{4.76}$$

Next we examine this situation for the case of a mismatch between the actions of the hostile nodes. As shown in Eqs. (4.77) and (4.78), if hostile node $h_1$ chooses action $b$ while hostile node $h_2$ chooses action $c$ or vice versa, the stealth utility of both nodes is decreased from 1 to $\delta_p \in [0, 1/2]$ where probability $p$ depends on the actions of the legitimate network L. Importantly we observe that this disadvantageous mismatch in actions actually corresponds to the direct attack. As illustrated in Figure 39a, when each hostile node attacks only one legitimate node the action mismatch is created. Thus we make two important conclusions. The first conclusion is that actions that constituted an equilibrium in the direct attack may no longer constitute an equilibrium in the cross attack. The second conclusion is that the cross attack

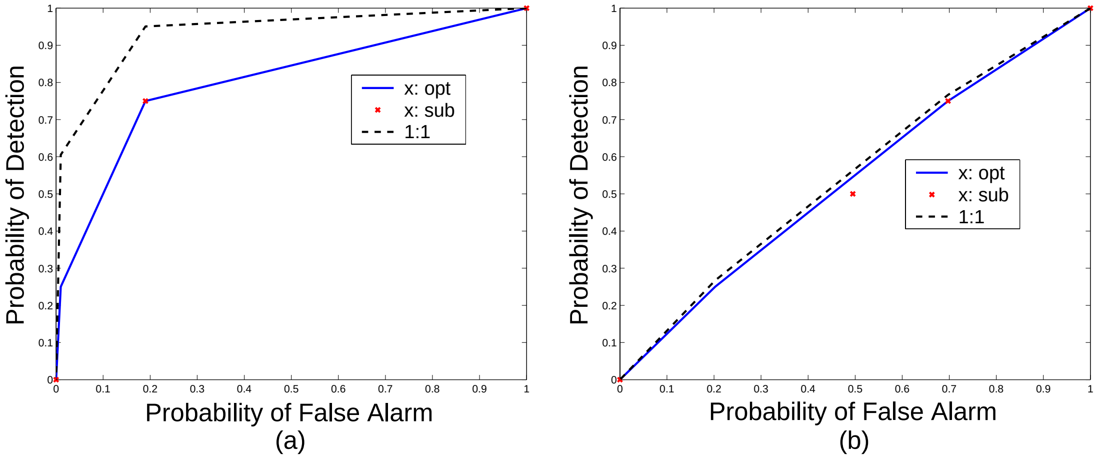


Fig. 40. Comparison of the direct and cross attacks for doublet $(b, c)$ for (a) $p = 0.1$. (b) $p = 0.45$.

achieves a superior level of relative stealth than the direct attack.

$$\mathcal{S}_c = u_2(q_2 = 1, q_3 = 0, \tilde{q}_2 = 0, \tilde{q}_3 = 1) = \delta_p \quad \in [0, 1/2] \tag{4.77}$$

$$\mathcal{S}_c = u_2(q_2 = 0, q_3 = 1, \tilde{q}_2 = 1, \tilde{q}_3 = 0) = \delta_p \quad \in [0, 1/2] \tag{4.78}$$

Next we proceed to examine the stealth utility for the doublet case when both hostile nodes mix their actions with equal probability based on Proposition 2. As shown in Eq. (4.79), such a mix is an equilibrium for the hostile nodes in the case of a cross attack and gives rise to a relative stealth of $1/2(1 + 1/3 \cdot \delta_p) \in [1/2, 7/12]$. We note that this equilibrium point did not exist in the case of the direct attack. The overall set of best response actions for hostile nodes $h_1$ and $h_2$ for this doublet scenario is shown in Eq. (4.80).

$$\mathcal{S}_c = u_2(q_2 = 1/2, q_3 = 1/2, \tilde{q}_2 = 1/2, \tilde{q}_3 = 1/2) = 1/2(1 + 1/3 \cdot \delta_p) \quad \in [1/2, 7/12] \tag{4.79}$$

$$B_1(\tilde{q}_2, \tilde{q}_3) = \begin{cases} q_2 = q_3 = 1/2 & \text{if} \quad \tilde{q}_2 = \tilde{q}_3 = 1/2 \\ q_2 = 1 & \text{if} \quad \tilde{q}_2 = 1/2 + \epsilon \quad \text{for} \quad \epsilon > 0 \\ q_3 = 1 & \text{if} \quad \tilde{q}_3 = 1/2 + \epsilon \quad \text{for} \quad \epsilon > 0 \end{cases} \tag{4.80}$$

To further illustrate the difference between the stealthy direct and cross attacks we obtain the absolute stealth of each attack at the cluster head in terms of the $P_D$-$P_{FA}$ performance. Figures 40a and 40b illustrate the results for the doublet pair $(b, c)$ and $(\tilde{b},\ \tilde{c})$ for both the optimal and sub-optimal detectors at the cluster head. As seen from these results, the cross attack achieves a worst $P_D$-$P_{FA}$ performance signifying that it is a better strategy for the attacker and is thus in agreement with the prediction of the stealth condition $\mathcal{S}_c$. Figure 41 illustrates this result for the case of a triplet cross attack as compared to a direct one-to-one attack. We summarize these results in remark 6.

**Remark 6** *The cross attack achieves a superior level of relative and absolute stealth compared to the direct attack for hostile network H.*

Importantly we observe that the above discussion encompassed only considerations of stealth and that the power of the attack $P_a$ was not jointly considered. To consider both metrics, we employ the power-communication-detection $PCD$ metric shown in Eqs. (4.81) and (4.82) and recall that communication among the hostile nodes may be accomplished via relatively simple algorithms such as Algorithm 3. Thus based on the $PCD$ metric we wish to compare the direct attack with the cross attack for both the case of communication and for the case of no communication among the hostile nodes.

$$PCD = \frac{\text{No. attacked nodes}}{(1 + \text{No. communications}) \cdot (1 + P_D)} \tag{4.81}$$

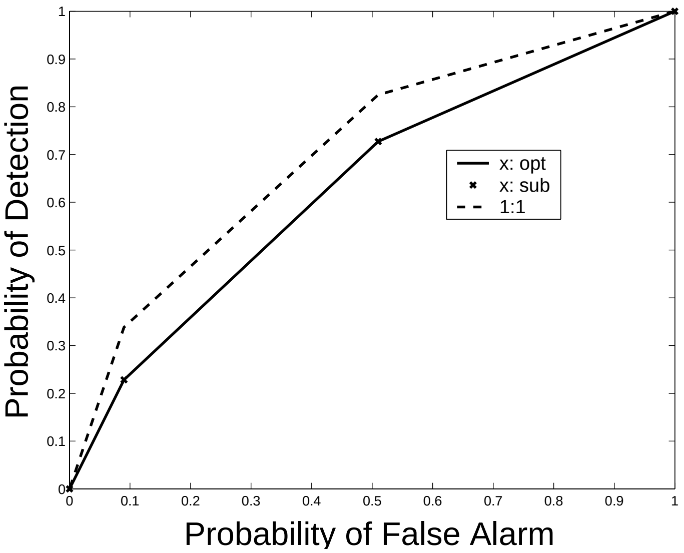


Fig. 41. Comparison of the direct and cross attacks for triplet $(a, b, c)$ for $p = 0.3$.

$$PCD_{Li} = \frac{Q_i}{1 \cdot (1 + P_D)} \tag{4.82}$$

The results of this comparison are shown in Table IX for the case of $n = 2$ nodes corresponding to the cross attack model where the results have been arranged in order of decreasing $PCD$ performance. As can be seen from the table, for the case of very small node subsets, the direct attack benefits from the use of inter-node communications as shown previously in Chapter III and Figure 27. As seen from the table however, the cross attack quadruplet strategy achieves a higher $PCD$ metric without the use of communications. Thus we obtain the result that for very small node subsets where two hostile nodes attack two legitimate nodes, it is advantageous for the hostile network to employ the cross attack quadruplet and that the hostile network does not need to employ inter-node communications to achieve this result.

Table IX. *PCD* Metric for Direct vs. Cross and Comm. vs. No Comm. for $n = 2$

| **Attack** | **Comm.** | **PCD** |
|---|---|---|
| direct | no | 0 |
| direct | yes | 0.1 |
| cross | yes | 0.195 |
| cross | no | 0.39 |

## 2. Comparison with Uncoordinated Attacks

In the previous section we compared the stealthy cross attack with the stealthy direct attack for the case of inter-node communication and for the case of no inter-node communication. We observed that the cross attack results in advantageous levels of stealth and power-communication-detection without the need for active communication. As noted in Section D-3 however, to achieve Nash equilibria in the cross attack without communication, the hostile nodes require knowledge of common priority lists as well as knowledge of all the nodes' positions. In this section we wish to investigate the implications of a mis-coordination on the part of the hostile nodes in achieving the Nash equilibria.

The case of mis-coordination among the hostile nodes is illustrated in Figure 42a in terms of the $P_D$-$P_{FA}$ performance at the cluster head for $p = 0.1$. Specifically, Figure 42a shows three types of deviation from the doublet equilibrium $(\mathbf{q}, \tilde{\mathbf{q}})$ where $\mathbf{q} = [1/2, 1/2, 0, 0]$ and $\tilde{\mathbf{q}} = [1/2, 1/2, 0, 0]$ corresponding to actions $(a, b)$ and $(\tilde{a}, \tilde{b})$. As can be seen from Figure 42a, the worst $P_D$-$P_{FA}$ performance from among the four curves is achieved precisely by the doublet equilibrium and thus constitutes the best case for H. When only one of the hostile nodes ($h_2$ in this example) deviates from this equilibrium by mixing with $\tilde{\mathbf{q}} = [1/4, 1/4, 1/4, 1/4]$, the result is a loss of stealth for

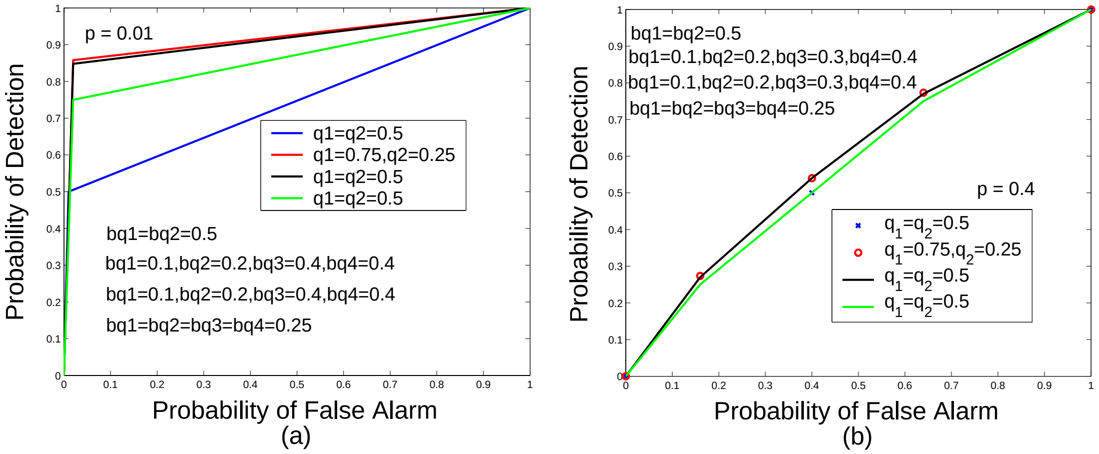


Fig. 42. $P_D$-$P_{FA}$ when $h_2$ deviates from optimal doublet mixing strategy for (a) $p = 0.1$. (b) $p = 0.4$.

H. Although significant, this loss is not maximal since $h_2$ has selected the quadruplet mixture which is generally advantageous for H.

Next we examine the stealth outcome when hostile node $h_2$ deviates from the doublet equilibrium mix by mixing among all four alternatives but in a way that does not correspond to the quadruplet equilibrium. Specifically, hostile node $h_2$ mixes using the strategy $\tilde{\mathbf{q}} = [1/10, 2/10, 3/10, 4/10]$. As can be seen from Figure 42a, this larger deviation from the equilibrium results in a larger loss of stealth for H. Finally we consider the case when both hostile nodes $h_1$ and $h_2$ deviate from the prescribed doublet strategy. In this scenario hostile node $h_1$ selects $\mathbf{q} = [3/4, 1/4, 0, 0]$ while hostile node $h_2$ selects $\tilde{\mathbf{q}} = [1/10, 2/10, 3/10, 4/10]$ as before. As can be seen from the figure, such mismatched selections result in the worst level of stealth for the hostile network H. Similar results of coordination mismatch are illustrated in Figure 42b but for the case where $p = 0.4$. We observe that the relationship between the four curves is maintained but that the gap in performance among the four is decreased. This is consistent with the finding that as the probability of an event $p$ approaches $p \approx 0.5$, the detection performance of the legitimate network decreases. Thus from the perspective of the hostile network, all attack strategies are comparable since the attack cannot be easily detected at the cluster head. Overall we observe that coordination among the hostile nodes for arbitrary values of probability $p$ is required and that smaller deviations from the optimal actions produce a smaller loss in stealth.

## F. Chapter Summary

In this chapter we investigated the competing sensor networks scenario for the case of a stealthy cross attack. In a stealthy cross attack, each hostile node may attack one or more legitimate nodes with some probability, causing an incorrect decision at the sensor. Unlike in the direct stealthy attack however, based on hostile node deployment and goals, two hostile nodes may both attack the same legitimate node. To understand the impact of the cross attack on reliable data collection, we investigated the stealth and power of the attack with comparisons to the direct attack for both networks.

The stealthy cross attack is modeled via the interaction between the hostile nodes in a static non-cooperative game. The stealth utility for this scenario is derived and shown to be consistent for both the hostile and the legitimate networks. Based on the stealth utility, the optimal attack and defense strategies are obtained for each network. For the hostile network, we showed that in contrast with the direct attack, multiple pure and mixed Nash equilibria exist. We showed that the pure equilibria are not advantageous for the hostile network and indeed may be considered a form of attack interference among the hostile nodes. We also showed that surprisingly there exist strategies for the cross attack in terms of mixed equilibria that achieve superior stealth for H than the direct stealthy attack without the need for communication. Furthermore there exists a unique attack strategy among the mixed equilibria which results in a superior power-communication-detection metric than the direct attack.

Importantly for the hostile network, we also showed that to achieve the desired Nash equilibrium in the cross attack based on coordination without communication, the hostile nodes require knowledge of common priority lists as well as knowledge of all the nodes' positions. Deviations from the prescribed coordination result in a loss of stealth.

For the legitimate network, we employed the derived stealth condition to obtain the best defense strategies. We showed how analysis of the cross attack enables use of established techniques to detect the attack such as through the Neyman-Pearson paradigm. We also showed that the optimal detection and mitigation strategies obtained for the stealthy direct attack apply to the stealthy cross attack and are thus consistent.

# CHAPTER V

# STEALTHY IMAGE NETWORK COMPETITION

## A. Introduction and Motivation

The general popularity of mobile devices and the lure of innovative applications have continued to drive research in the area of wireless multimedia. Indeed much focus has been placed on the design of robust, efficient and secure schemes for delivering multimedia content over error-prone wireless channels [98], [99]. Recent years have also brought developments in another growing field of interest, that of wireless sensor networks. Originally envisioned as simple devices for distributed environmental sensing, sensor networks have continued to evolve in complexity to include autonomous mobility and actuation of elements in their surroundings [100], [101]. Visual-capability additions are thus but a natural extension of this research [92], [102].

Emerging from these ideas, the nascent field of wireless image sensor networks (WISNs) considers battery-operated wireless (untethered) nodes equipped with cameras [92], [102]. Among other applications, it boasts importance to rapid-deployment surveillance and monitoring [10]. As all ambitious research ideas, WISNs have many significant challenges to overcome. The energy limitations already encountered in sensor networks collecting scalar data such as temperature are only exacerbated when nodes are deployed to collect, process and transmit visual data [103], [104]. The increased size of visual data also strains storage buffers and places a further burden on system design through increased transmission delay and bandwidth utilization [16]. Such challenges require innovative solutions tailored to the unique characteristics of WISNs [92].

Among possible approaches, event driven WISNs have emerged as an intriguing design possibility suited for long term deployments in unattended environments. In the event driven approach, camera nodes may be triggered by scalar sensors only when the latter detect an event of interest in the surroundings. Alternative event driven approaches consider cameras that acquire continuous input but which only transmit an image frame if an event was captured [16], [50]. The event driven paradigm hence aims to alleviate energy consumption and bandwidth use implicitly, via the local selection of relevant image frames by the nodes. This approach may be viewed as complementary to the joint optimization of video encoding and wireless transmission power [99], [103], or to efforts at providing higher bandwidth channels [10] and allocating their use fairly and efficiently [98]. Overall, WISN systems will undoubtedly benefit from the incorporation of advances from the spectrum of these complementary strategies.

Event acquisition and frame selection in the event driven paradigm may be accomplished through the use of scalar sensor decisions and the use of image processing techniques at the camera nodes. At the camera nodes, many event driven WISN paradigms rely on correct frame selection based on the definition of an event. For surveillance nodes where unknown objects may or may not enter the camera's field of view, this definition may be largely motion-based, though in general the definition is application-dependent [105], [106]. Based on the event definition, a camera node should ideally achieve a high probability of event detection $P_D$ to guarantee that important frames are acquired and transmitted. The camera nodes should also achieve an acceptably low probability of false alarm $P_{FA}$ to avoid the wasteful acquisition or transmission of non-event frames. Event detection in WISNs must thus meet critical accuracy and reliability requirements while minimizing complexity and energy consumption. Though approaches based solely on image processing at the camera nodes are possible, they are generally expensive in terms of the computation required to achieve an acceptable probability of error [103], [104].

In this work we show how collaborative approaches exploiting available scalar decisions can be used in conjunction with low complexity image processing algorithms to achieve reasonable performance despite the potential presence of a hostile network. Based on the competing sensor networks scenario with stealthy direct or cross attacks, we examine the event acquisition properties of WISNs deployed in unattended outdoor environments for the purpose of collecting relevant surveillance data regarding an event of interest [6], [43].

We consider a heterogeneous WISN comprised of sensors and untethered camera nodes (battery operated nodes with wireless data transmission to the sink) [3]. The camera nodes must operate reliably under significant resource constraints and may thus require the use of lightweight image processing (LIP) algorithms to perform event acquisition [7], [102]. Under the collaboration paradigm, camera nodes may also receive supporting decisions about the presence or absence of an event from distributed sensors [102], [16]. We wish to investigate the detection and false alarm characteristics of such heterogeneous WISNs in uncertain environments where outdoor conditions may present challenges for the camera LIP algorithms while occasional faults and deliberate stealthy attacks may present a challenge for the supporting sensors. In particular we wish to study the relative merits and limitations of the following cases:

1. Lightweight Image Processing (LIP) approach: preliminary results from real-world testbeds of low-power low-computation wireless camera nodes suggest that LIP algorithms may achieve a probability of detection and false alarm ($P_D$-$P_{FA}$) that may be acceptable for certain applications [7], [102]. Though we do not set out to improve any particular LIP algorithm, in this work we wish to

understand the underlying analytical properties of simple threshold based LIP algorithms and examine their $P_D$-$P_{FA}$ performance for a variety of real world surveillance sequences. The overarching goal is thus to understand the limits and suitability of LIP algorithms and to provide a framework for enhancing their performance with sensors if required for a given application.

2. Sensor Decisions Approach: in unattended outdoor settings, sensors may be prone to occasional errors due to faults or may experience stealthy direct or cross attacks designed to avoid detection [6], [31], [43]. Although quality testing may provide an estimate for the probability of a fault, an estimate for the probability of an attack may not be generally available a priori. Without verification mechanisms, the reliability of the sensor decisions may thus not be adequate for some applications despite node redundancy. We study and compare the $P_D$-$P_{FA}$ performance of different fault/attack verification mechanisms at the cluster head for the case of occasional errors, attacks and stealthy attacks. We also comment on the level of node redundancy (cluster size) required to achieve a desired event acquisition performance under each scenario.

3. Combined Decisions Approach: camera nodes may rely on a combination of decisions from the sensors and the LIP algorithm for event acquisition [7], [102], [3]. We wish to study the characteristics of such combined decisions for various levels of node redundancy to exploit the desirable qualities of both approaches and avoid the degradation in performance that each method may experience in certain settings.

## B. Literature and Recent Advances

For many applications, the viability of wireless image sensor networks (WISNs) depends on the resolution of significant design issues centered around network reliability [49], [107] longevity [22], [103] and security [108], [109]. The specific issues include energy-efficient capture of images as well as their processing and routing [110], [102], [111], [112], economical network design relying on node heterogeneity with sleep/wake-up cycles [113], [3], and the network's robustness to attack and compromise of privacy [114]. WISNs thus present a very wide range of timely challenges. In this section we wish to briefly outline some recent advances most salient to the focus of our work.

In [3] He *et. al* describe VigilNet, a prototype implementation of a heterogeneous image sensor network for energy efficient surveillance missions. In the experimental setup, 70 Mica2 motes are deployed to detect and track the passing of a vehicle while triggering cameras. The authors demonstrate how a multi-tier sleep/wake-up system consisting of motes and mote leaders called sentries can extend the lifetime of the network. Importantly, a sentry decides whether an event of interest is occurring in the environment by counting the number of "yes" votes it receives from the motes which are utilizing magnetometer sensors. To accurately capture events, the probabilities of false positives and false negatives are balanced by carefully selecting the detection threshold (i.e. the number of "yes" votes required to declare that an event has occurred, referred to by the authors as the Degree of Aggregation DoA). Importantly, the DoA is selected *experimentally* and as the authors suggest, a framework with adjustable sensitivity for this selection could largely improve the system's detection performance. In comparison, in our work we study a framework that enables the cluster head (i.e. the sentry) to make optimal decisions based on sensor inputs with a flexible level of sensitivity.

Although heterogeneous multi-tier systems greatly improve the longevity of the *overall* image network, practical designs must account for the substantial power consumption of individual image-capture devices and of their image processing algorithms which handle the acquired frames. Recent advances in CMOS imaging technology have produced a new breed of low-power camera devices. Unfortunately these devices are generally intended for higher-power hosts and are thus not suitable for sensor networks. To address this issue, Rahimi *et. al* [7] present a seminal camera device named Cyclops. Cyclops provides an electronic interface between a low-power low-computation camera module based on CMOS imagers and a lightweight camera host such as a mote. While providing a critical bridge and enabling use in visual sensor networks, Cyclops still suffers from extreme constraints in its computational power and processing delay, necessitating judicious use of its resources. For instance, Cyclops's complex programmable logic device (CPLD) can perform simple operations on the frames at *capture time*, such as background subtraction and frame differentiation. Performing such simple operations at capture time instead of post-processing the frames greatly reduces the energy consumption and delay of the device. In our work, we study how lightweight image processing (LIP) compatible with these ideas can improve event detection performed by the cluster head and its associated sensors. Importantly cyclops indeed possesses an asynchronous trigger input that can be connected to sensors (such as a passive IR detector, microphone or magnetometer) to trigger the camera and improve the overall system's performance.

Upon deployment, the goal of a typical image network is to *capture relevant* visual surveillance pertaining to an event of interest and to forward this surveillance to a sink where further analysis might be performed. To capture relevant surveillance, the network should generally exhibit a high probability of event detection $P_D$ (true positive) and a low probability of false alarm $P_{FA}$ (false positive). These probabilities not only affect the relevance of the collected materials to the surveillance task, but also have an impact on the network's energy consumption and thus on its longevity. Specifically, the erroneous identification of "non-event" frames as "significant" and their subsequent processing and transmission through a (wireless) medium needlessly drains the nodes' battery resources and burdens the sink with non-content. On the other hand, the omission of "event" frames may significantly compromise the quality of the surveillance mission. The $P_D$-$P_{FA}$ characteristics of the image network should also ideally exhibit the highly desirable property of being adjustable based on the requirements of the application (such as its surveillance or energy requirements). The detection performance should also ideally exhibit some optimality in the sense of being "the best" achievable performance given the practical challenges of WISNs.

Event acquisition challenges experiences by nodes in a WISN generally stem from more than one source. The first such source originates from the hardware and energy limitations of the camera nodes themselves [7]. Specifically, the camera nodes may not have the *capability* of applying advanced image processing to the captured frames. The processing delay (per frame) as well as the energy and memory utilization generally render such processing infeasible even when it is available at the camera nodes. However lightweight image processing (LIP) is often feasible on such devices and provides very basic *in situ* analysis of the frames' content. Unfortunately the practical $P_D$-$P_{FA}$ performance of LIP varies widely depending on the specific environmental conditions (for example, lighting, size and speed of the moving object(s) and movement of "background" objects such as trees). The performance of LIP for any given arbitrary image sequence is consequently not truly predictable or controllable, and thus not inherently "adjustable" to meet application requirements. Nevertheless, real-world experiments with Cyclops based on a LIP algorithm have demonstrated an average $P_D \approx 78\%$ and a $P_{FA} \approx 22\%$ [7]. While this level of $P_D$-$P_{FA}$ performance may potentially be acceptable for certain applications, it is important to investigate whether this performance can be improved through the use of collaborating sensors.

Exploiting the information collected by sensors might generally improve the $P_D$-$P_{FA}$ performance of heterogeneous WISNs. The use of sensors however introduces two new sources of error that must be considered. The first such source comes from occasional sensor faults or errors that occur with some small but non-zero probability at each sensor. Aside from quality testing prior to deployment (which might be selective or altogether absent due to the large number of sensors), the general approach is to employ sensor *redundancy* to reduce the chance of false reporting. Nevertheless it is not always clear what *level of redundancy* (number of sensors) is required to achieve a given $P_D$-$P_{FA}$ performance, especially if the camera nodes are already performing a basic level of detection via a LIP algorithm. The issue of redundancy becomes even more salient when we consider the second possible source of sensor error, that is, error due to a persistent and distributed attack. In particular, WISNs are intended for deployment in unattended and possibly hostile regions. In such scenarios, an opponent can clearly gain physical access to the sensors with the possibility of destroying them, capturing them for reprograming purposes, or interfering with their readings via actuator devices [49], [6]. Despite the possibility of tampering or error, the use of sensors to achieve reliable and energy efficient image networks is highly enticing if these issues can be resolved [92], [7].

## C. System Model

We investigate the WISN event acquisition problem in uncertain environments where the sensors are prone to either occasional faults or stealthy hostile attacks and where the camera devices perform very basic event detection using lightweight image processing (LIP) algorithms with unpredictable performance due to varying conditions. Specifically we wish to understand how the role of sensor redundancy changes if uncertainty in the environment shifts from mere faults to hostile attacks. For instance we wish to understand if LIP algorithms alone are sufficient in certain cases (such as the case of a severe sensor attack) or if their performance should be augmented with that of sensors.

In this section we wish to detail the specific system setup analyzed in this work. As shown in Figure 43, a camera node has the capability of performing lightweight image processing (detailed in Section D) to perform event acquisition. The camera node may however also rely on input from one or more (error or attack-prone) sensors regarding the presence or absence of an event of interest (shown in Figure 43 as binary “yes/no” decisions). Information from the sensor(s) may be directly fed into the camera or it may first pass through a cluster head (CH) where a form of attack/error detection is performed. In that case, the camera node receives a decision about the presence or absence of an event from the cluster head instead of directly from the sensor(s).

Based on this setup, a camera node may receive information about the presence or absence of an event from more than one source (i.e. from the sensor(s)/cluster head and from its own frame processing). Since it is not known a priori which source will be more reliable under a given setting, the camera node faces several possible methods of utilizing the received information. Specifically, the camera node must decide which source to trust when the sources are in disagreement (i.e. one source reports an event of interest while the other reports no event). As shown in Table X, one possible approach to resolve a disagreement is for the camera to trust its lightweight image processing (LIP) as the more “reliable” element which is not prone to attack. Indeed

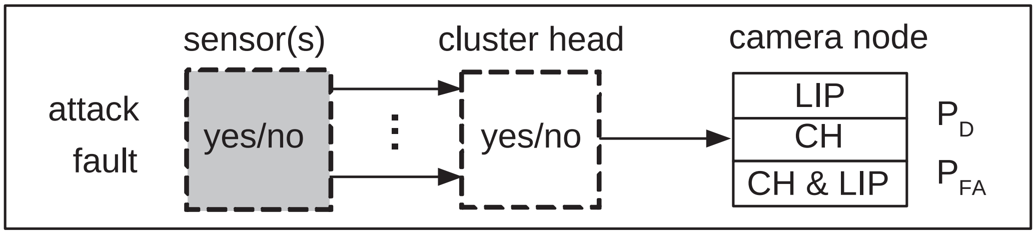


Fig. 43. Each camera node may employ lightweight image processing (LIP) to determine if an event of interest has occurred in a collected frame or it may rely on decisions from the sensor(s)/cluster head (CH) or a combination of both (CH & LIP).

such a strategy might be fruitful in favorable lighting and background-motion conditions. Another obvious approach is for the camera node to trust the sensor/cluster head decision (CH in Table X) and treat the LIP as the more volatile element. Finally the third approach listed in Table X instructs the camera to mark a frame as an "event" if *either* of the two sources reports an event. This approach *may* prevent the missed detection of certain events but could produce many false reports if at least one of the sources experiences significant errors. Thus under arbitrary environmental conditions, it is not clear which of the techniques will produce a better *overall* $P_D$-$P_{FA}$ performance (with $P_D$ as close to 1 as possible and $P_{FA}$ as close to 0 as possible) and how sensor redundancy will affect this performance.

Based on the model of Table X and based on the sensor and optimal attack

Table X. Methods for Marking a Frame As an "Event" at Camera Node

| **Method** | **Action for Marking Frame as an Event** |
|---|---|
| LIP | Mark based on Lightweight Image Processing (LIP) |
| CH | Mark based on sensor(s) with/without Cluster Head (CH) detection |
| CH & LIP | Mark if *either* LIP *or* CH detects an event |

models from Chapters III and IV, the competition between the two networks for the case of visual event acquisition in unattended envrionments is summarized in definition 9.

**Definition 9** *The stealthy competition between networks $H$ and $L$ for the case of image networks is defined by the following network goals:*

- *$H$ network: perpetrate stealthy (direct or cross) attack so as to misguide the visual event acquisition of the legitimate network's camera nodes.*
- *$L$ network: achieve a desired $P_D$-$P_{FA}$ visual event acquisition performance at the camera nodes given lightweight image processing and the potential presence of stealthy attacks on the sensors.*

Finally we make an important note regarding the use of notation for the case of attacks in competing image networks. In the case of image networks, we employ the notation $q$ in a very broad sense to denote the probability of a scalar sensor error. This sensor error may be caused by occasional faults, attacks or stealthy direct or cross attacks. In comparison, we previously employed the notation $q$ to denote the stealthy direct attack exclusively. In the broader case currently considered, the sensor error could be the result of a variety of sources. We employ the familiar $q$ notation for simplicity and convenience while keeping in mind its broadened meaning.

## D. Analysis for Event Acquisition

In this section we wish to examine the visual event acquisition process at the camera nodes. We begin with an examination of the characteristics of real-world surveillance sequences and proceed to analyze the properties of a representative threshold-based visual detector. Finally we obtain the practical $P_D$-$P_{FA}$ performance of the detector

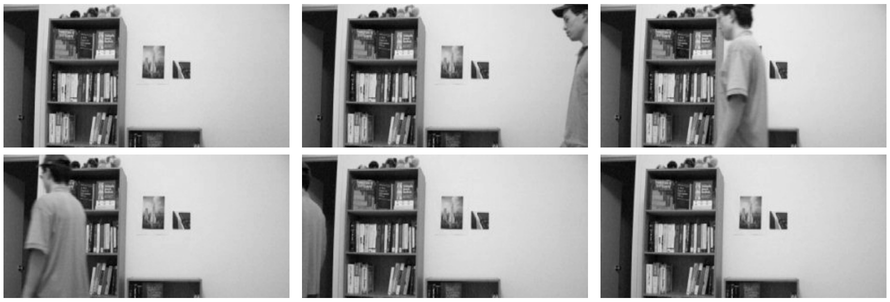


Fig. 44. Frame Seq. 1: indoor test conditions with constant lighting and no background changes.

and compare it with existing results from practical implementations of image sensor networks.

### 1. Image Sequence Characteristics

In the spirit of lightweight image processing (LIP) [7], [115], [116], we consider a relatively simple and general event acquisition algorithm (i.e. the approach is not tailored to the detection of any *specific* type of object). Examination of the proposed algorithm is intended to provide more insights into the properties of simple visual algorithms and serve as an illustration of their performance in the context of energy and computation-limited camera nodes. To assess this generic algorithm for WISNs we consider its properties in analytic form and obtain the algorithm's $P_D$-$P_{FA}$ performance for surveillance sequences under varying conditions. The real-world image sequences used in our testing are shown in Figures 44, 45, 46, and 47. The characteristics of these sequences are important in understanding the suitability of the proposed algorithm for event acquisition in WISNs. We thus describe the test sequences prior to outlining the visual event acquisition algorithm.

The sequence of Figure 44 is an idealized indoor test where the lighting and background conditions do not change appreciably over time. The only significant change comes from the event of interest in the form of a test subject entering the

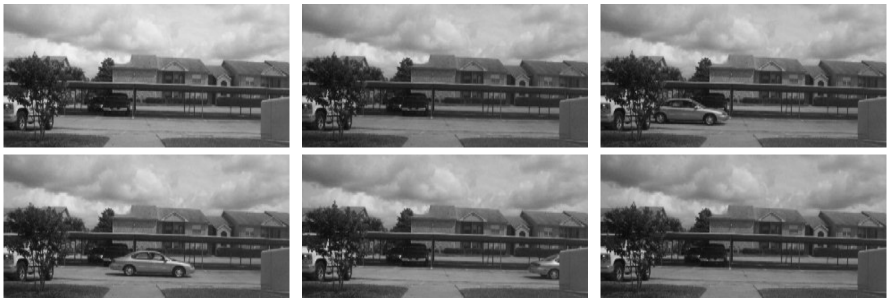


Fig. 45. Frame Seq. 2: outdoor variable lighting due to clouds. The light intensity changes by 70% between frames. Additional background movement due to shrub.

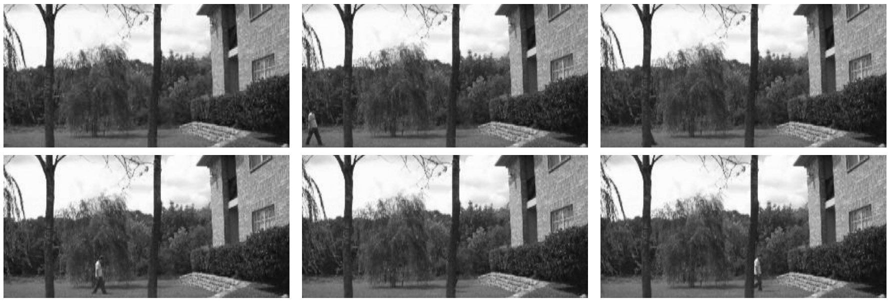


Fig. 46. Frame Seq. 3: changing outdoor light and background (swaying trees). The subject temporarily disappears behind a tree.

camera's field of view. The dominant source of noise in this case is internal camera noise and flicker. The sequence of Figure 45 shows outdoor parking-lot surveillance on a windy day, where the event of interest is the passing of an unidentified car. The event acquisition task in this sequence is complicated by the presence of a nearby shrub which experiences significant swaying of its branches over time. Furthermore the background lighting changes visibly with cloud movement. The sequence of Figure 46 also experiences changes due to swaying trees and variable light conditions. The event of interest is the appearance and movement of a test subject which temporarily disappears behind a tree in frames 4c and 4e. Finally Figure 47 shows a truncation

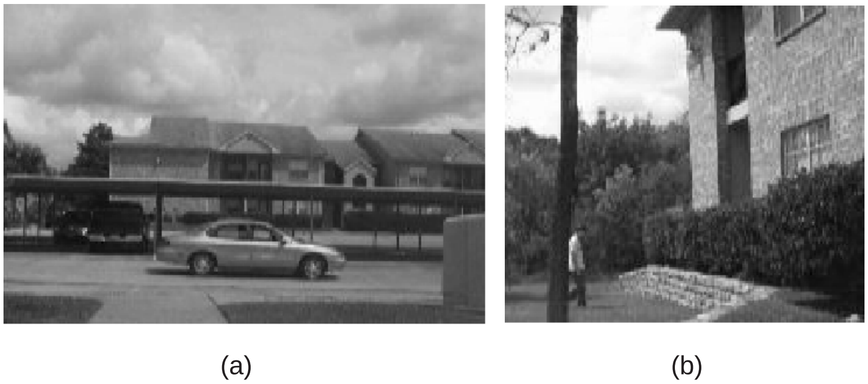


Fig. 47. (a) Frame Seq. 4a showing Seq. 2 modified to remove the shrub. (b) Frame Seq. 4b showing Seq. 3 modified to remove the swaying trees.

of the sequences of Figures 45 and 46 where the camera's field of view now excludes the shrub and trees.

Statistical analysis of the image sequences in Figures 45 and 46 (such as Levine's Test and the t-test) reveal that the mean and standard deviation are not reliable indicators of an event of interest occurring even after various (DCT domain) filtering mechanisms are employed. This can be seen intuitively from the fact that the subjects of interest (person walking and car driving-by) do not occupy a much larger percent of a frame's pixels than the other randomly moving objects (shrub and trees). Hence the mean and variance of the frames *do* change based on the appearance of the subject, but these differences are not statistically distinguishable. In essence, the pixels corresponding to the person and car are getting dwarfed by the presence of many shrub and tree pixels which are also changing over time. Truncating the frames as shown in Figure 47 to exclude the vegetation does indeed improve the statistical difference between an event and non-event frame. However for the general WISN deployment case (with cameras facing in various directions), we do not wish to select an event acquisition technique which relies on the truncated assumption. Based on the observed statistical similarity of event and non-event frames, we wish to determine an event detector suitable for WISNs. In addition to its generality (detection not tailored to a specific type of object) and good detection performance, the chosen event detector should be implementable in the simple WISN devices. In addition to their hardware and general processing limitations, WISNs process a large volume of surveillance frames which must in turn be transmitted wirelessly to the sink if they contain an event of interest. Analysis of frames at the small block or pixel level may consequently not always be suitable or possible.

Instead we seek a simple form for the detector where a single frame statistic is compared to a threshold in order to determine the presence or absence of an event. However as discussed, event and non-event frames from real-world surveillance sequences have similar statistics. Furthermore it can be shown (Appendix B) that a difference image $D = B - A$ computed from two consecutive frames $A$ and $B$ is not perfectly Gaussian but rather contains significant outliers (this is shown for both event and non-event frames). An optimal non-parametric (robust) detector is thus more appropriate for this case of statistical similarity and presence of outliers. However we show that a simple chi-squared detector (relying on a comparison of a frame statistic to a threshold) is *equivalent in form* to the robust detector and can thus be used in WISNs. Furthermore, through the use of composite hypothesis testing, we show that the chi-squared detector can be made uniformly most powerful (UMP) through proper threshold selection. The UMP property signifies that the detector achieves a probability of detection $P_D$ *higher or equal to* the detection of all other detectors given the worst-case scenario probability of false alarm $P_{FA}$. In other words, no detector performs better given the same probability of false alarm.

## 2. Lightweight Image Processing for Event Acquisition

The simple algorithm we selected is based on difference images, similar to the techniques found in the image change detection literature [117]. We describe this detector, which we refer to as the "chi-squared" detector, as an adaptation of the detector proposed by Aach and Kaup [105], [118], where we use entire difference frames instead of blocks. We now overview the basics of the technique. In essence, a difference image $D = B - A$ between two consecutive frames $A$ and $B$ reveals all the pixels that have changed between these frames containing both relevant and irrelevant changes (such as the tree swaying). The Mean Squared Error (MSE) of the difference image is computed as the relevant statistic, and it is compared to a theoretically-obtained robust threshold $T$. We now present the specific details of this detector.

In Aach and Kaup [105], [118] (and in Radke *et al.* [117]), the difference image $D$ is computed and divided into smaller blocks. Importantly, each pixel of the *difference* image is modeled as a Gaussian random variable with 0 mean and variance $\sigma_i^2$, where $i = 0$ corresponds to a non-event frame and $i = 1$ corresponds to an event frame. In order to conserve computational energy, in this work we use the entire difference image instead of parsing the image to determine salient blocks. The resulting detector hypothesis test can be summarized as:

$$\mathcal{H}_0 \;:\; \text{no event, } D_k \sim \mathcal{N}(0, \sigma_0^2)\ \forall k \tag{5.1}$$

$$\mathcal{H}_1 \;:\; \text{event, } D_k \sim \mathcal{N}(0, \sigma_1^2)\ \forall k \tag{5.2}$$

with $\sigma_0^2 < \sigma_1^2$ and where $D_k$ is the $k^{\text{th}}$ difference pixel in $D = B - A$. Since the entire difference image is utilized in the detection, instead of considering individual pixels we may consider a new random variable defined as:

$$X \;=\; \sum_{k=1}^{n} D_k^2 = \sigma_j^2 \sum_{k=1}^{n} \frac{D_k^2}{\sigma_j^2} = \sigma_j^2 Y, \quad \text{for j} \in \{0,1\} \tag{5.3}$$

where $Y$ has distribution chi-squared with $n$ degrees of freedom and where $n$ is the total number of pixels in the difference frame. The new detection hypothesis test is thus given by:

$$\mathcal{H}_0 \;:\; X \sim \frac{1}{\sigma_0^2} f_{\chi^2,n}\left(\frac{x}{\sigma_0^2}\right) \tag{5.4}$$

$$\mathcal{H}_1 \;:\; X \sim \frac{1}{\sigma_1^2} f_{\chi^2,n}\left(\frac{x}{\sigma_1^2}\right) \tag{5.5}$$

where $f_{\chi^2,n}(x)$ is the probability density function (pdf) of the chi-squared distribution with $n$ degrees of freedom. Significantly, the hypothesis test to distinguish between an event and non-event is given by the comparison of a single statistic ($x$) to a threshold $T$ as shown in Eqs. (5.6) and (5.7), where $\sigma_0^2$ is the variance of a null frame, $f_{\chi^2,n}^{-1}$ is the inverse chi-squared distribution and $\alpha$ is the desired probability of false alarm.

$$x \underset{H_0}{\overset{H_1}{\gtrless}} T \tag{5.6}$$

$$T = \sigma_0^2 f_{\chi^2,n}^{-1}(1-\alpha) \tag{5.7}$$

### 3. Lightweight Event Acquisition Properties

In this section we wish to analyze some of the properties of the simple chi-squared detector of Eqs. (5.6) and (5.7) and examine its practical performance on the surveillance test sequences. We begin by showing that the simple chi-squared detector can be made uniformly most powerful (UMP) [96]. To achieve this we show that if there exists a real positive number $\gamma$, such that $\sigma_0^2 < \gamma$ and $\sigma_1^2 > \gamma$, where the actual $\sigma_0^2, \sigma_1^2$ are *unknown*, then there exists a UMP detector where a realization $x$ from Eq. (5.3) is compared to a threshold $T$, such that the probability of false alarm $P_{FA} = \alpha$ is given by:

$$\alpha = \sup_{\sigma_0^2 < \gamma} \int_T^\infty \frac{1}{\sigma_0^2} f_{\chi^2,n}\left(\frac{x}{\sigma_0^2}\right) dx \tag{5.8}$$

Suppose there exists a $\gamma > 0$, such that $\sigma_0^2 < \gamma$ and $\sigma_1^2 > \gamma$ in Eqs. (5.4) and (5.5). Then there exists a UMP test of the form

$$x \underset{\mathcal{H}_0}{\overset{\mathcal{H}_1}{\gtrless}} \gamma f_{\chi^2,n}^{-1}(1-\alpha) \tag{5.9}$$

for false alarm rate not exceeding $\alpha$. This is a composite hypothesis test in which the parameters for the null and alternate hypotheses are unknown, but the regions for these parameters are divided by a threshold $\gamma$. The proposition says that if the parameter space is divided as thus, then a test that compares the actual $x$ in Eq. (5.3) to a threshold, achieves optimal detection when the worst case false alarm is considered (the use of sup in Eq. (5.8)).

If we can show that the likelihood ratio is monotonically increasing in $x$ for $\sigma_1^2 > \sigma_0^2$, then the UMP test of the form in Eq. (5.9) follows from a theorem on composite hypothesis testing [96]. It can easily be shown that the log-likelihood ratio is given by

$$\frac{1}{2}\left(\frac{1}{\sigma_0^2} - \frac{1}{\sigma_1^2}\right) x + \frac{n}{2} \ln\left(\frac{\sigma_0^2}{\sigma_1^2}\right).$$

Since $\sigma_1^2 > \sigma_0^2$, this ratio is strictly increasing in $x$. To show that $T$ is as given on the left side of Eq. (5.9), we note that the probability of false alarm is given by $1 - f_{\chi^2,n}(T/\sigma_0^2)$ by applying an integration change of variable in Eq. (5.8). To get the sup in Eq. (5.8), it suffices to set $\sigma_0^2 = \gamma$.

Having established that the simple detector of Eq. (5.6) and (5.7) can be made uniformly most powerful, we next show that the form of the detector is equivalent to that of a robust (non-parametric) detector. This is an important property given that the statistical similarity of event and non-event frames along with difference-frame distributions that are not quite Gaussian render $\mathcal{H}_1$ and $\mathcal{H}_0$ almost indistinguishable when the entire frame is used. Thus we would like to maximize the event detection assuming that $\sigma_1^2 \approx \sigma_0^2$ rather than assuming that the statistics are significantly different. This can be re-phrased as

$$\max \frac{\partial \beta}{\partial \sigma_1^2}|_{\sigma_1^2=\sigma_0^2} \tag{5.10}$$

where $\beta = Pr\{\text{declare } H_1 \mid H_1 \text{ occurs}\}$ is the probability of detection.

The test

$$x \underset{H_0}{\overset{H_1}{\gtrless}} T \tag{5.11}$$

maximizes Eq. (5.10) for a false alarm rate not exceeding $\alpha$, i.e. $T$ is chosen so that

$$\alpha > \int_T^\infty \frac{1}{\sigma_0^2} f_{\chi^2,n}\left(\frac{x}{\sigma_0^2}\right) dx. \tag{5.12}$$

By the proof of the Neyman-Pearson lemma [96], the optimal test can be shown to be of the form

$$\frac{\frac{\partial \frac{1}{\sigma_1^2} f_{\chi^2,n}\left(\frac{x}{\sigma_1^2}\right)}{\partial \sigma_1^2}\Big|_{\sigma_1^2=\sigma_0^2}}{\frac{1}{\sigma_0^2} f_{\chi^2,n}\left(\frac{x}{\sigma_0^2}\right)} \underset{H_0}{\overset{H_1}{\gtrless}} \tilde{T}, \tag{5.13}$$

which is equivalent to

$$\frac{x - n\sigma_0^2}{2\sigma_0^4} \underset{H_0}{\overset{H_1}{\gtrless}} \tilde{T}. \tag{5.14}$$

Letting $T = 2\sigma_0^4 \tilde{T} + n\sigma_0^2$ finishes the proof.

In summary, given the actual statistics of the difference image, a non-parametric (robust) detector is appropriate to perform event detection. However the simple chi-squared detector is equivalent in form to the robust detector and can be made uniformly most powerful through threshold selection. The simple image difference test may thus be used at the camera nodes with acceptable performance within its class of algorithm complexity.

### 4. Lightweight Event Acquisition Performance

Given these desirable properties, we would like to examine how the visual event acquisition algorithm performs on the real-world surveillance sequences described in Section 1. Table XI shows the performance results obtained for these sequences arranged in order of *decreasing* performance. We make several key observations regarding these results. The first observation is that the *median* performance result (corresponding to Seq. 2 is quite similar to the results obtained in [7] despite differences in the form of the exact LIP algorithm that is utilized (in [7] the average reported $P_D = 0.78$ compared with our $P_D = 0.87$ and the average reported $P_{FA} = 0.22$ compared with our $P_{FA} = 0.26$). This result is encouraging in that Seq 2 corresponds to an unknown object moving in difficult outdoor conditions with significant lighting changes and the presence of extraneous motion. Thus despite their simple nature, LIP algorithms for event acquisition do hold some promise. The second observation from Table XI is that the *actual* $P_D$-$P_{FA}$ performance varies greatly depending on the specific image sequence. It is thus very difficult to guarantee a given level of performance in the camera node for an *arbitrary* sequence.

If we classify the image sequences into broad categories based on their characteristics, a coarse level of performance prediction may be possible. For instance, sequences with minimal levels of extraneous motion achieve a better overall performance than sequences afflicted with such motion. Sequences where an object occupies a larger portion of the overall frame (such as a car rather than a person) also show

Table XI. Event Detection Based on Lightweight Image Processing (LIP) Organized in Order of Decreasing Detection Performance $P_D$

| **Image Sequence** | **Description** | $\mathbf{P_D}$ | $\mathbf{P_{FA}}$ |
|---|---|---|---|
| Seq. 1 | Indoor walking | 1.0 | 0.13 |
| Seq. 4a | Outdoor car (no trees) | 0.98 | 0.17 |
| Seq. 2 | Outdoor car (with trees) | 0.87 | 0.26 |
| Seq. 4b | Outdoor walking (no trees) | 0.50 | 0.03 |
| Seq. 3 | Outdoor walking (with trees) | 0.05 | 0.23 |

improved $P_D$-$P_{FA}$ performance[1]. Though intuitive, these observations do not provide much assistance for the general WISN case where camera nodes may encounter conditions that vary appreciably over time. We thus seek a collaborative approach between camera nodes equipped with LIP algorithms and sensors to help capture the value of visual detection while addressing the large variability in its performance.

## E. Performance and Comparisons

As discussed in Section D, lightweight image processing (LIP) may offer a suitable $P_D$-$P_{FA}$ performance for event acquisition in WISNs. This performance however exhibits significant variability depending on the conditions experienced during image capture. To exploit the potential of LIP algorithms while reducing their variability, we wish to augment the event acquisition process with sensors. Sensors however are prone to occasional faults or deliberate stealthy attacks as studied in Chapters III and IV. We may thus consider a variety of methods at the camera nodes for exploiting the sensor

[1] This conclusion extends to real-world sequences with multiple moving objects. Indeed the presence of multiple moving objects tends to improve motion-based detection. The single moving object may thus be viewed as a worst-case scenario in certain cases.

decisions and the LIP algorithm to improve reliability as discussed in Section C. In this section we wish to explore the implications of utilizing a cluster head fault/attack detector mechanism before making the sensor decisions available to the camera nodes. Based on this input, the camera nodes may trust the sensor decisions, the LIP decision or rely on a combination of both. For perspective, we wish to compare this scenario with the case where sensor decisions are made available directly to the camera nodes *without* a cluster head fault/attack detection mechanisms.

### 1. Direct Sensor Decisions Approach

In this section we focus on the $P_D$-$P_{FA}$ performance of a camera node augmented with a single sensor decision that is made directly available to the camera node as depicted in Figure 48. Thus to perform event acquisition under this scenario, a camera node has access to two sources of information regarding the possible occurrence of an event. As shown in Figure 48, if there is disagreement between the two sources regarding the presence of an event, the camera node may trust the lightweight image processing (LIP) over the potentially faulty or attack-prone sensor. Alternatively, the camera node may trust the sensor decision (SN) in lieu of the variability-prone LIP algorithm or may take the "safe" strategy of declaring an event if *either* of the sources reports an event.

$$P_D = \frac{\text{No.(event|event frame)}}{\text{No.(total frames)}} \tag{5.15}$$

$$P_{FA} = \frac{\text{No.(event|non-event frame)}}{\text{No.(total frames)}} \tag{5.16}$$

Figures 49 and 50 show the simulation results obtained for this scenario where we use the notation IM to denote (lightweight) image processing, SN to denote the sensor decisions and "sensor & IM" to denote use of the combination. Figure 49a depicts the results obtained for the image sequence of Figure 46 where an unidentified

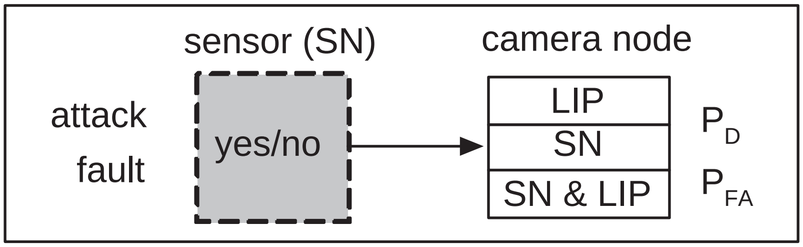


Fig. 48. For event acquisition, each camera node may utilize lightweight image processing (LIP), a sensor decision (SN), or rely on both to determine the presence or absence of an event.

individual walks through an environment with substantial background movement and is periodically obscured due to the presence of trees. Figure 49b shows the results for a truncated version of this sequence corresponding to Figure 47b where the camera's field of view largely excludes the trees. Figure 50a shows the results for the image sequence of Figure 45 where the passing of an unknown vehicle is captured in the presence of significant background variability. Finally Figure 50b shows the results obtained for a truncated version of the passing car and corresponds to the image sequence depicted in Figure 47a. Importantly, the horizontal axes in Figures 49 and 50 correspond to the probability $q$ of sensor error (due to attack or fault) and the vertical axes correspond to the probability of detection $P_D$. The resulting probability of false alarm for the sensor $\alpha_s$ is also shown in the figures for each $P_D$ segment along with the probability of false alarm for the LIP algorithm $\alpha_{IM}$. These probabilities are obtained experimentally based on Eqs. (5.15) and (5.16) where No. denotes the number of frames where a certain type of decision was made.

Based on Figures 49 and 50 we confirm that the $P_D$-$P_{FA}$ performance of the lightweight image processing exhibits great variability from sequence to sequence. As expected, this performance tends to improve for image sequences with better

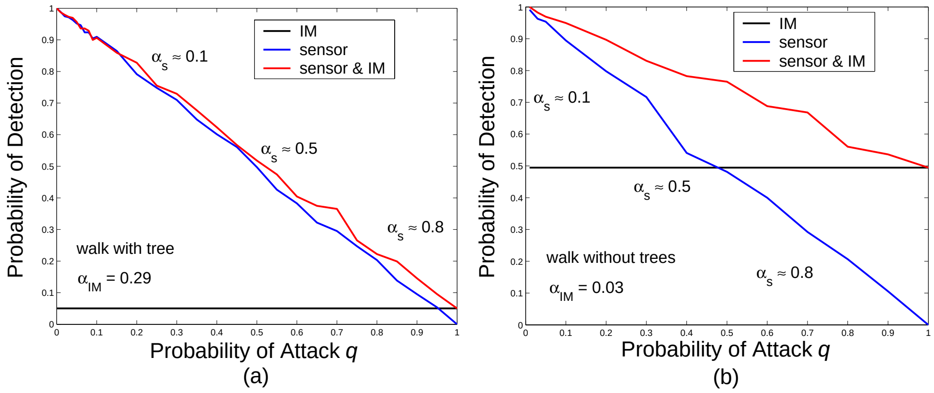


Fig. 49. Probability of detection $P_D$ vs. probability of sensor error $q$ for the LIP, SN and SN & LIP approaches for sequence (a) walk with trees from Figure 46. (b) walk without trees from Figure 47b.

characteristics (such as less background variability). The level of improvement itself however experiences variability as can be seen by comparing Figures 49a and 49b with Figures 50a and 50b. We also note the inherent result that the probability of detection $P_D$ and the probability of false alarm $P_{FA}$ for the image processing algorithm remain constant over the entire range of $q$. This is fully expected since the visual algorithm at the camera node is independent of the sensor readings. The lack of predictability and control in the LIP algorithm for an arbitrary sequence is a visible disadvantage. However the constancy of the LIP performance over the range of $q$ is a clear advantage as can be seen by comparing the SN and SN & LIP curves in Figures 49 and 50.

Specifically, the $P_D$-$P_{FA}$ performance of the single sensor is excellent for a *small* probability of error $q$. However if this probability of error is caused by an attack, it may become arbitrarily large and dramatically decrease the event acquisition performance (the performance decreases linearly with increasing $q$). Indeed in this setup the sensor does not perform a fault/attack detection and therefore an attacker *need not be stealthy* in the attack, but rather choose *any* implementable probability of attack $q$. The combined SN & LIP approach however inherits the best of both approaches;

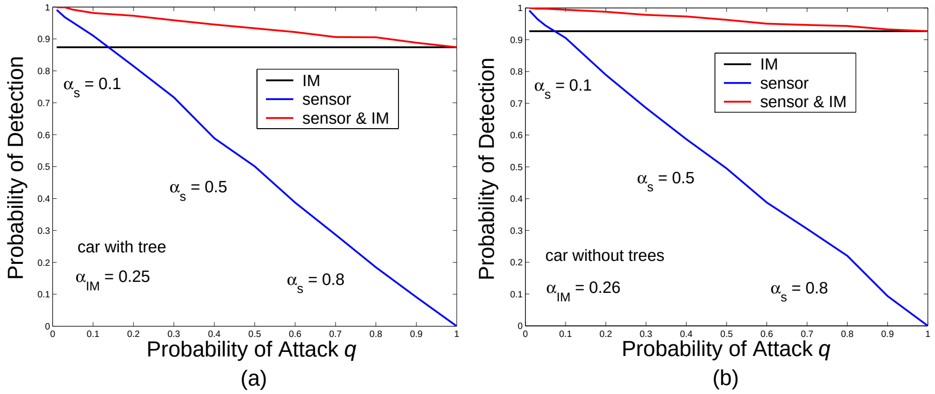
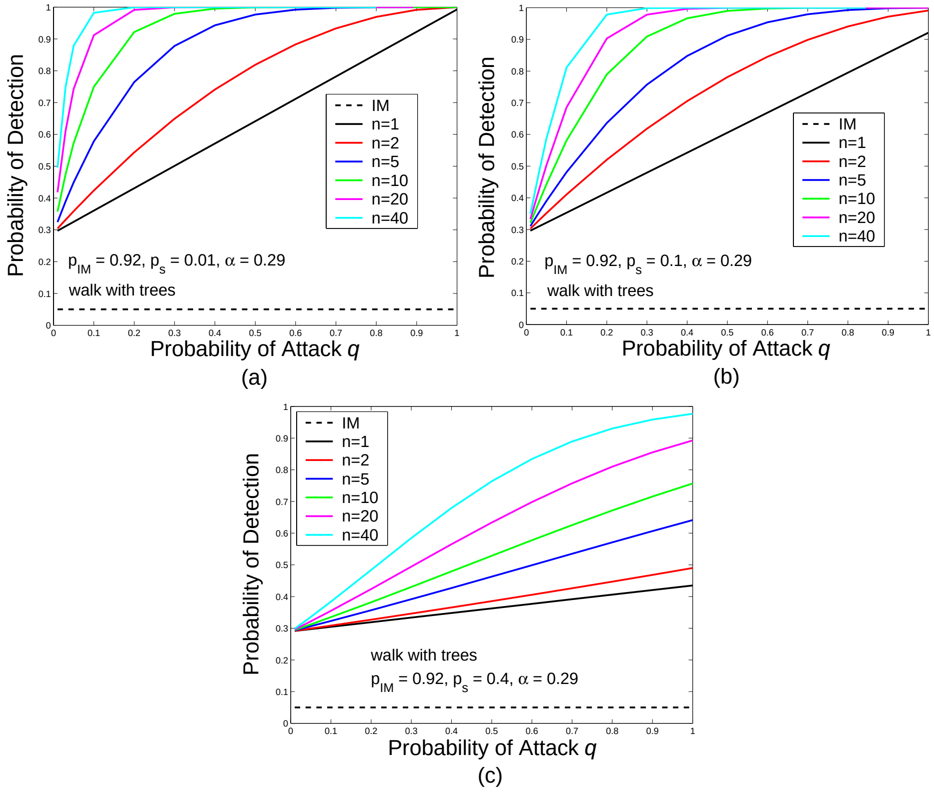


Fig. 50. Probability of detection $P_D$ vs. probability of sensor error $q$ for the LIP, SN and SN & LIP approaches for sequence (a) car with trees from Figure 45. (b) car without trees from Figure 47a.

the good performance of the sensor given a small $q$ and the invariance of the LIP approach over the range of $q$. Thus we observe that the $P_D$-$P_{FA}$ performance of the combined approach is always *better than or equal to* the *best* performance from among the other two methods. Specifically, for a fixed probability of false alarm $P_{FA}$, the probability of detection $P_D$ of the combined approach is described by Eq. (5.17). It is important to note that the probability of false alarm of the sensor $\alpha_s$ varies depending on $q$. Thus for a direct comparison of $P_D$ with the LIP, we have to locate the point on the SN & LIP curve where $\alpha_s \approx \alpha_{IM}$ in order to obtain the result of Eq. (5.17) (as can be seen from the figures however, the SN & LIP curves lie above the LIP curve for all values of $q$).

$$P_{D_{\text{combined}}} \geq \max(P_{D_{\text{LIP}}}, P_{D_{\text{SN}}}) \tag{5.17}$$

Since combining the LIP with a *single* sensor decision *without* cluster head checking improves the performance in uncertain environments, it is important to determine if including cluster head checking and increasing the number of sensors results in a justifiably improved level of performance. Indeed the performance achieved with the "direct sensor approach" may be sufficient for certain applications.



(a)

(b)

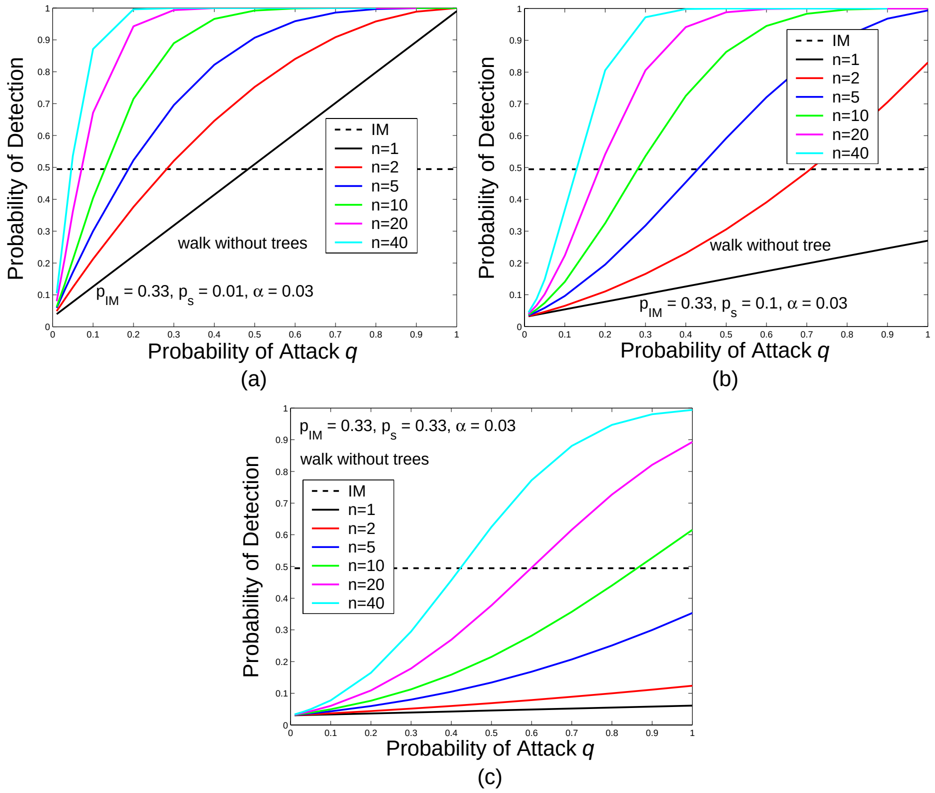
(c)

Fig. 51. $P_D$ v.s. $q$ for walking with trees from Figure 46. (a) $p_s = 0.01$. (b) $p_s = 0.1$. (c) $p_s = 0.4$.

## 2. Cluster Head Aided Event Acquisition

In this section we wish to investigate the role of cluster head (CH) checking based on the detectors presented in Chapters III and IV, as well as the role of sensor redundancy $n$ in improving the $P_D$-$P_{FA}$ performance in uncertain environments.

We begin by comparing the relative performance of the LIP algorithm with the performance of the CH detector (based on decisions from $n$ sensors). Figure 51 shows the event acquisition performance of multiple sensors *with* cluster head detection and corresponds to the image sequence of an individual walking with the presence of trees. As before the horizontal axis represents the probability of attack $q$ while the vertical axis corresponds to the probability of detection $P_D$. The probability of detection $P_D$



(a)

(b)

(c)

Fig. 52. $P_D$ v.s. $q$ for walking without trees from Figure 47b. (a) $p_s = 0.01$. (b) $p_s = 0.1$. (c) $p_s = 0.33$.

of the LIP algorithm for each sequence is also shown in the figures for comparison and all probabilities are determined experimentally from Eqs. (5.15) and (5.16). As before, the notation IM denotes the image processing (LIP) based performance. The number of sensors $n$ reporting their decisions to the cluster head is varied from $n = 1$ to $n = 40$.

In assessing the relative performance of the LIP algorithm and the CH detector with $n$ sensors in Figures 51-52 we maintain the *same* probability of false alarm $\alpha$. That is, we set $\alpha_s = \alpha_{IM} \triangleq \alpha$. In contrast, in Section E-1 a single sensor was used instead of a CH detector. Thus the probability of false alarm $\alpha_s$ was not adjustable but rather varied with the attack parameter $q$.

Figure 52 corresponds to the image sequence of the individual without the back-

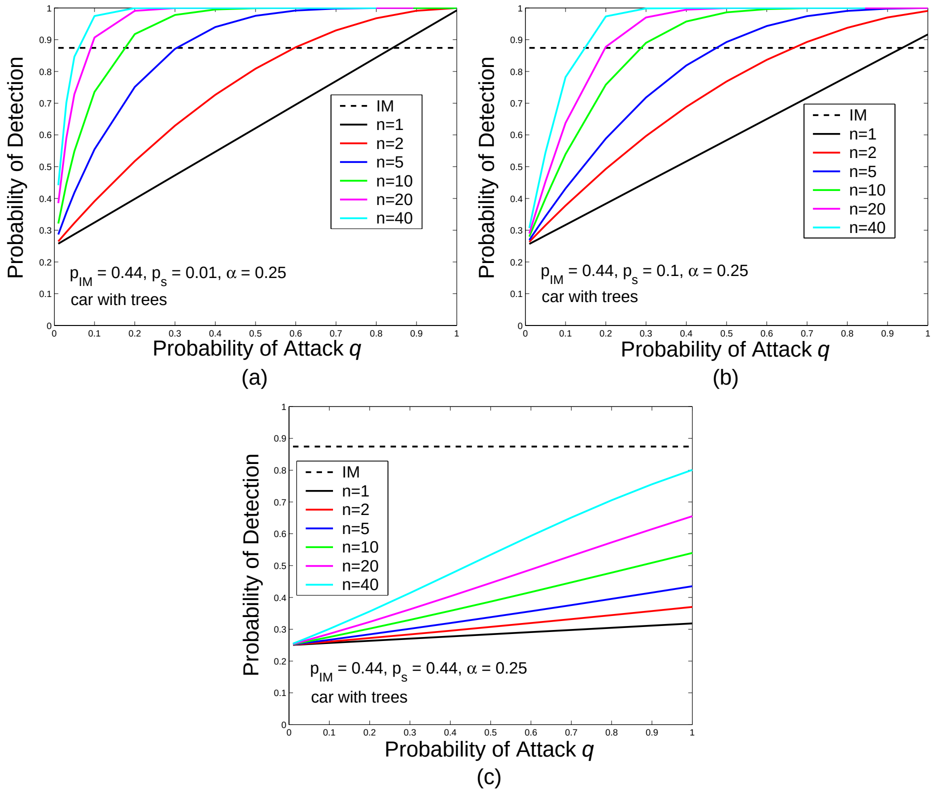


Fig. 53. $P_D$ v.s. $q$ for car with trees from Figure 45 (a) $p_s = 0.01$. (b) $p_s = 0.1$. (c) $p_s = 0.44$.

ground trees. Furthermore we use the notation $p_s$ to denote the probability $p$ of an event as witnessed by a sensor (the subscript $s$ is used to emphasize that this probability corresponds to the conditions experienced by the sensor). We use the notation $p_{IM}$ to denote the probability that a *frame* in a given image sequence contains an event. In Section E-1, $p_s$ was implicitly set to $p_{IM}$, however in this section we relax this constraint to investigate the role of the probability of an event at a sensor $p_s$ as well as the role of cluster size $n$.

The first key point is that use of the CH detector fundamentally changes the relationship between the probability of detection $P_D$ and the probability of sensor error $q$. Specifically, use of the CH detector eliminates the linear decrease in sensor performance with increasing $q$. Indeed the sensors achieve a better detection perfor-

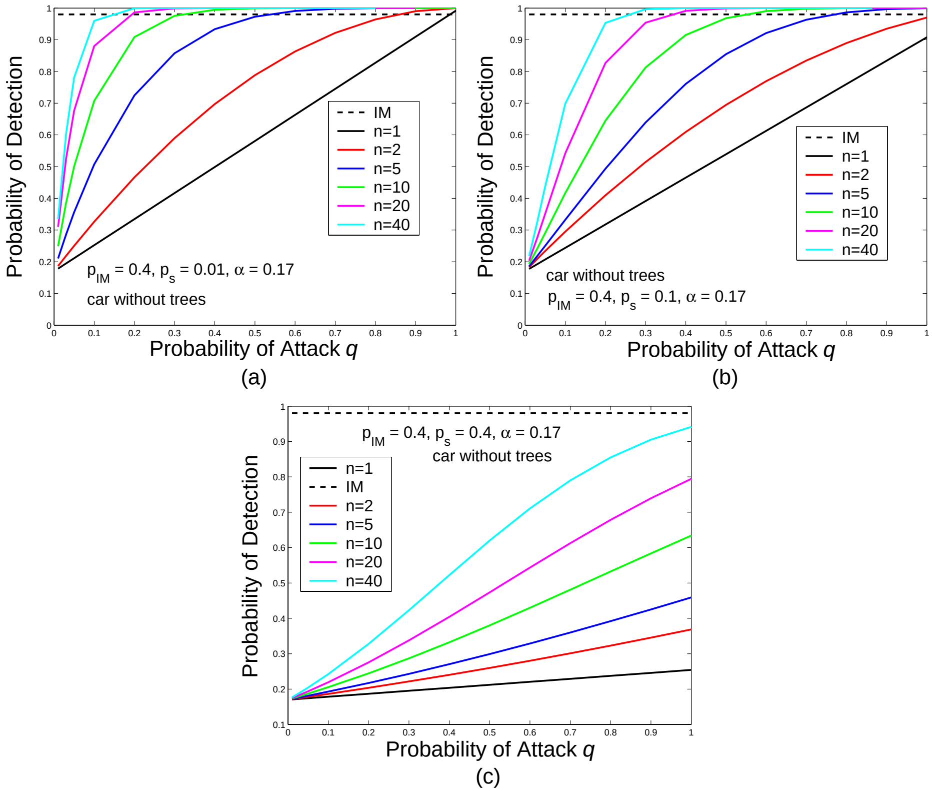


Fig. 54. $P_D$ v.s. $q$ for car without trees from Figure 47a (a) $p_s = 0.01$. (b) $p_s = 0.1$. (c) $p_s = 0.44$.

mance for higher values of $q$ which also results in a relatively good $P_D$ over a much wider range of $q$. This result is an inherent outcome of the properties of detectors which perform better when there is a significant difference between the hypotheses (in this case the values of probabilities $p_s$ and $q$). Use of the detector will thus increase the detection performance for the case of unstealthy attacks (i.e. attacks with a large probability $q$ relative to the cluster size $n$). This is in contrast with the results of Section E-1 where an increase in $q$ degraded the detection performance.

Figure 53 corresponds to the car sequences with the presence of trees while Figure 54 corresponds to the car sequence without background trees. Unfortunately use of the detector alone (without LIP) for the case of very small $q$ (such as due to stealthy attacks or occasional errors) may not be sufficient, and as evidenced in the plots of

Figures 51-54, may necessitate the use of a higher value of $n$.

The second key observation is that choosing a threshold $T_h$ that results in a smaller probability of event $p_s$ results in a better sensor performance (in accordance with the results of Chapters III and IV). Indeed for a small value of $p_s$, it may be possible to obtain the desired $P_D$-$P_{FA}$ performance with a smaller number of sensors $n$. As can be seen by comparing parts a, b, and c of Figures 51-54, choosing $p_s = 0.01$ (part a) offers a better performance than setting $p_s = 0.1$ (part b). Thus in general we do not wish to set $p_s = p_{IM}$ (part c) since $p_{IM}$ may be arbitrarily large depending on the image sequence. Finally we observe that for certain values of $p_s$ and $n$, the lightweight image processing algorithm (LIP) still achieves a better detection performance for certain values of $q$ than the CH detector.

Based on these results we now wish to investigate the performance of a camera decision that is based on combining the CH detector with the LIP algorithm. Figure 55a shows the $P_D$ v.s. $q$ performance for the image sequence of an individual walking in the presence of trees (from Figure 46) while Figure 55b depicts this performance for the truncated walking sequence (from Figure 47b). Figure 56a shows the performance for the image sequence of a vehicle in the presence of trees (from Figure 45) while Figure 56b depicts this performance for the truncated car sequence (from Figure 47a).

In Figures 55a, 55b, 56a and 56b, the dashed lines represent the performance based on the CH detector alone while the solid lines represent the performance of the combined decisions. As can be seen from these figures, the combined decisions achieve a better (or equal) detection performance $P_D$ (for the same probability of $\alpha$) than the CH decisions or the LIP decisions alone. This is consistent with the results obtained in Section E-1 (where a single sensor decision was utilized without CH detection). However by utilizing the CH detector, we avoid the degradation of the detection performance for large $q$ while by utilizing the LIP algorithm we avoid

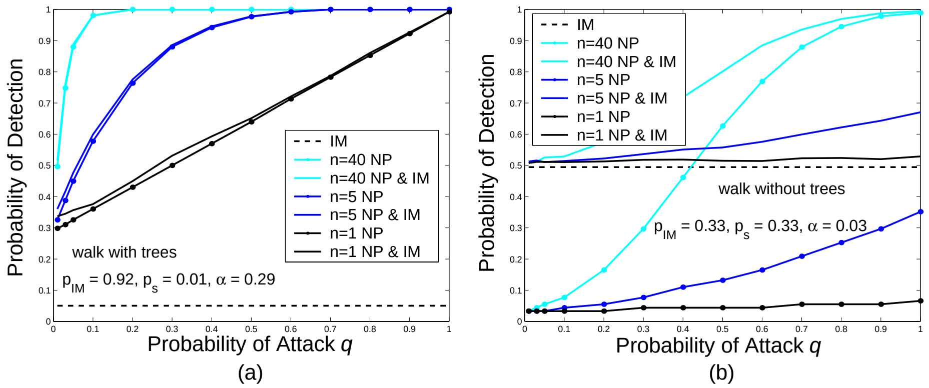


Fig. 55. (a) $P_D$ v.s. $q$ for walking sequence *with* tree from Figure 46 for $p_s = 0.01$. (b) $P_D$ v.s. $q$ for walking sequence *without* tree from Figure 47b for $p_s = 0.33$.

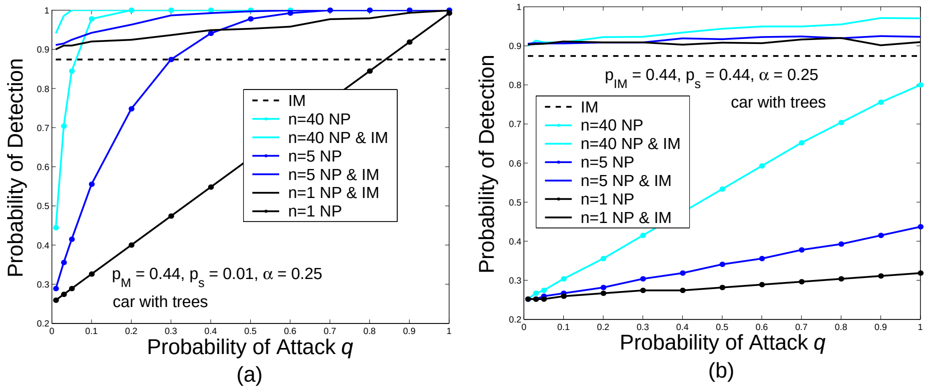


Fig. 56. $P_D$ v.s. $q$ for car sequence with tree from Figure 45 for (a) $p_s = 0.01$. (b) $p_s = 0.44$.

the degradation of detection for small $q$. Thus based on the selection of a suitably small $p_s$ and/or the selection of a suitably large cluster size $n$, we are able to adjust the $P_D$-$P_{FA}$ performance to suit the application requirements over the entire range of error $q$ due to error or attack.

## F. Chapter Summary

Wireless image sensor networks (WISNs) consisting of untethered camera nodes and sensors may be deployed in a variety of unattended and possibly hostile environments to obtain surveillance data. In such settings, the WISN nodes must perform reliable event acquisition to limit the energy, computation and delay drains associated with forwarding large volumes of image data wirelessly to a sink node.

In this work we investigated the event acquisition properties of WISNs that employ various techniques at the camera nodes to distinguish between event and non-event frames in uncertain environments that may include stealthy attacks. These techniques include lightweight image processing, decisions from $n$ sensors with/without cluster head fault and attack detection, and a combination approach relying on both image processing and sensor decisions. In closing, we summarize the resulting properties and observations for event acquisition in WISNs:

1. Lightweight Image Processing (LIP) Approach in Uncertain Environments:

   a. LIP algorithms are generally compatible with low-power, low-complexity camera nodes [7]. Indeed analysis demonstrates that simple LIP algorithms (such as based on the comparison of a single frame statistic to a threshold) have the same form as robust and UMP detectors which motivates their use.

   b. The typical probabilities of detection and false alarm obtained in our experiments were consistent with the average probabilities reported in the literature with our $P_D = 0.87$ and our $P_{FA} = 0.26$.

   c. While achieving an average $P_D$-$P_{FA}$ performance that may be suitable for some applications, the LIP algorithm exhibited large *variability* in its performance from sequence to sequence depending on environmental conditions. LIP algorithms alone thus may not offer the level of performance control and flexibility required in many applications.

2. Sensor Decisions Approach in Uncertain Environments:

a. Sensors deployed in unattended outdoor environments may be prone to occasional faults or deliberate attacks that may be carried out in a stealthy manner (i.e. such as to avoid detection). Although quality testing may provide an estimate for the probability of a fault, an estimate for the probability of an attack may not be generally available a priori. Without verification mechanisms, the reliability of the sensor decisions may not be adequate for some applications.

b. An optimal Neyman-Pearson (NP) fault/attack detector based on the comparison of a single statistic to a threshold can be implemented at the cluster head to verify the sensor decisions. Based on the results of Chapter III, a detector where the comparison threshold is based on the average expected weight (i.e. the count or degree of aggregation) can also be implemented. This detector follows the performance of the NP detector closely, especially for small values of the probability of an event $p$.

c. For the case of stealthy attacks, use of a cluster head (CH) detector forces the attacker to select a smaller probability of attack $q$, especially for a larger cluster size $n$. This has the dual effect of rendering attacks more rare but also harder to detect despite the ability to predict the optimal attack parameter as given in the analysis of Chapter III. The attacker can also improve the stealth and power of the attack by applying a stealthy cross attack strategy as analyzed in Chapter IV. Such strategies by the attacker necessitate the use of verification mechanisms at the cluster head including the use of LIP algorithms.

3. Combined LIP and Sensor Approach:

a. For the case of *no* cluster head attack/fault verification, combining a single sensor decision with a decision based on a LIP algorithm does provide an improved event acquisition performance. Specifically, for a fixed probability of false alarm, the combined decision achieves a probability of detection $P_D$ higher than or equal to the $P_D$ of LIP and SN over the entire range of the probability of sensor error $q$. Although better than LIP or SN alone, the detection performance does decrease with increasing $q$, which without cluster head detection, may be arbitrarily large depending on the attacker.

b. Combining decisions from $n$ sensors with cluster head verification and LIP decisions provides the best overall performance over the entire range of attack probability $q$. Specifically, by utilizing the CH detector we avoid the degradation of the detection performance for large $q$ while by utilizing the LIP algorithm we avoid degradation of detection for small $q$.

c. Choosing a sensor threshold $T_h$ that results in a smaller probability of event $p_s$ (depending on the underlying sensor technology) results in a better sensor performance and allows the use of a smaller cluster size $n$ to achieve the desired $P_D$-$P_{FA}$ performance.

# CHAPTER VI

# CONCLUSIONS AND FUTURE WORK

## A. Conclusions

In this work we investigate the data *collection* process in a sensor network at the physical layer for the case of competing sensor networks. The networks are deployed in a common environment where one of the networks is hostile and perpetrates the attack in a distributed manner. In comparison with previous studies, we explicitly model the attack as an active competition between the two sensor networks. In addressing the problem we overcome the challenges that arise from the pervasive nature of the attack, the possibility of tampering during data acquisition prior to encryption and the lack of prior knowledge regarding the characteristics of the attack. We investigate the competing networks scenario for both the case of a direct stealthy attack and the case of a stealthy cross attack in scalar and image sensor networks.

In the direct stealthy attack each hostile node may attack a legitimate node with some probability chosen such that the overall stealth of the hostile network is maintained. The persistence and pervasiveness of the attack throughout the cluster causes incorrect individual sensor decisions as well as errors in the collective decision at the cluster head. The competitive interaction between the two networks is modeled as a game $\mathcal{G}$ where we derive a stealth condition $\mathcal{S}$ and show its consistency and relevance for both the hostile and the legitimate network in terms of attack detection and mitigation. For the hostile network H we show how the stealth condition can be utilized to select the optimal attack parameter for cases where the cluster size $n$ and the sensor threshold $T_h$ of the legitimate network L may not be known. For the legitimate network L we show how the stealth condition yields the optimal defense parameters in terms of $n$ and $T_h$ and how this analysis enables the use of established detection tools such as the Neyman-Pearson paradigm. In general, the optimal attack parameter decreases with increasing cluster size $n$ and with decreasing probability of an event $p$. While this improves attack mitigation by restricting the power of the attack $P_a$, it also makes the attack less detectable at the cluster head and thus presents a detection-mitigation trade-off for the legitimate network.

Importantly the direct stealthy attack does not require active communication among the hostile nodes during the attack but rather depends on a level of coordination which we quantify. Compared with the active communications case, we show that the stealthy direct attack achieves a higher power of attack $P_a$ and a higher power-communication-detection $PCD$ metric for certain cases. Importantly, the direct stealthy attack exhibits a constancy in the power of attack $P_a$ with respect to the cluster size $n$ that may be mistaken for inherent sensor faults and is thus highly desirable for stealth.

Finally we note the role that encryption plays in the competing networks scenario. Forward encryption between the sensors and the sink cannot protect against a hostile attack due to its occurrence during data collection. Based on the role of the sensor threshold $T_h$ in the stealth game, it is the backward encryption between the sink and the sensors that plays a role in attack mitigation and discovery.

In a stealthy cross attack, each hostile node may attack one or more legitimate nodes with some probability, causing an incorrect decision at the sensor and an incorrect overall decision at the cluster head. Unlike in the direct stealthy attack however, based on hostile node deployment and goals, two hostile nodes may both attack the same legitimate node. The stealthy cross attack is modeled via the interaction between the hostile nodes in a static non-cooperative game $\mathcal{G}_c$. The stealth utility $\mathcal{S}_c$ for this scenario is derived and shown to be consistent for both the hostile and the legitimate networks. Based on the stealth utility, the optimal attack and defense strategies are obtained for each network.

For the hostile network, we show that in contrast with the direct attack, multiple pure and mixed Nash equilibria exist. The resulting pure equilibria are not advantageous for the hostile network and indeed may be considered a form of attack interference among the hostile nodes. Surprisingly, there exist strategies for the cross attack in terms of mixed equilibria that achieve superior stealth for H than the direct stealthy attack without the need for communication. Furthermore there exists a unique attack strategy among the mixed equilibria which results in a superior power-communication-detection $PCD$ metric than the direct attack. Importantly for the hostile network, to achieve the desired Nash equilibrium in the cross attack based on coordination without communication, the hostile nodes require knowledge of common priority lists as well as knowledge of all the nodes' positions. Deviation from the prescribed coordination results in a loss of stealth.

For the legitimate network, we employed the derived stealth condition $\mathcal{S}_c$ to obtain the best defense strategies. We show how analysis of the cross attack enables use of established techniques to detect the attack such as through the Neyman-Pearson paradigm. Importantly, the optimal detection and mitigation strategies obtained for the stealthy direct attack apply to the stealthy cross attack and are thus consistent.

In addition to scalar data acquisition, sensor networks may be deployed in a variety of unattended and possibly hostile environments to obtain visual surveillance data. Such wireless image sensor networks (WISNs) may consist of untethered camera nodes and sensors where the latter may be prone to stealthy direct or cross attacks. In such settings, the WISN nodes must perform reliable event acquisition to limit the energy, computation and delay drains associated with forwarding large volumes of image data wirelessly to a sink node. For the case of such WISNs, we investigate event acquisition properties based on various techniques at the camera nodes to distinguish between event and non-event frames during hostile distributed attacks. These techniques include lightweight image processing (LIP), decisions from $n$ sensors with or without cluster head attack detection, and a combination approach relying on both image processing and sensor decisions.

Interestingly we confirm that simple LIP algorithms based on the comparison of a single frame statistic to a threshold have the same form as robust and UMP detectors which motivates the use of such LIP algorithms. Importantly, while achieving an average $P_D$-$P_{FA}$ performance that may be suitable for some applications, LIP algorithms generally exhibit large variability in their performance from sequence to sequence depending on environmental conditions. LIP algorithms alone thus may not offer the level of control and flexibility required in many applications.

On the other hand, sensor decisions (SN) may be prone not only to occasional errors but rather to pervasive stealthy attacks. In the case of such stealthy attacks, increasing the cluster size $n$ reduces the power of the attack but renders attack detection more challenging and thus constitutes a trade-off for the legitimate network L. We show that when decisions from the $n$ sensors are combined with attack detection at the cluster head and with LIP decisions, the complementary characteristics of the LIP and SN techniques result in a superior event acquisition performance. Specifically, use of the cluster head detector prevents performance degradation for the case of a large probability of sensor error while use of the LIP algorithm prevents performance degradation in the regime of a small probability of sensor error. Overall, cluster head detection along with cluster size $n$ and threshold $T_h$ selection allow the legitimate network L to achieve a desired $P_D$-$P_{FA}$ event acquisition performance in uncertain environments.

## B. Future Work

In this work we investigate a new and insidious form of attack on sensor network data at the physical layer of collection. The attack affects a sensor node prior to the encryption, encoding and verification processes. As such it necessitates the study of attack and defense mechanisms presented in this work. Without suitable detection and mitigation schemes, the effects of the attack can be particularly detrimental to rapid-deployment untethered visual sensor networks. For such untethered networks (battery-operated with wireless-transmission), it may be fruitful to couple the study of actuation attacks with other known sensor network security attacks. Such a study might be particularly insightful when actuation attacks are considered jointly with radio-jamming denial of service attacks. Indeed the stealthy actuation attack might be considered a form of denial of service, where the attack affects the *sensing* rather than the *transmission* activities. Joint jamming and actuation strategies could be analyzed to yield trade-offs between the effectiveness of the attack, the utilized energy and the resulting attack stealth. Such analysis would help to guide future sensor network architecture and security design to most effectively secure the network given available resources.

In terms of attack modeling, we note that the current abstraction captures the effects of the attack upon the decisions of the scalar sensors. The alteration of decisions through actuation is modeled as a binary symmetric channel where the probability of altering a decision from $0 \to 1$ is the same as the probability of altering a decision from $1 \to 0$. Such a model is useful in the current study where we do not wish to restrict the analysis to a specific type of actuator. Given knowledge of the characteristics of a specific type of actuator, a binary asymmetric channel model could be adopted and yield further insights.

Further extensions of this work may consider an alternative interpretation of the hostile network. Instead of interpreting the hostile network as a foreign entity, we may interpret the hostile network as formed from a set of *malicious* nodes *inside* the *legitimate* network. This is a common scenario investigated by sensor network security researchers. In such a scenario, a node belonging to the legitimate network becomes malicious when it is captured and reprogrammed by an outside entity for nefarious purposes. When several such nodes are captured, they may form a hostile sub-network within the legitimate network based on their programming. If active communication among the subverted nodes is not allowed, the hostile nodes may require a framework for distributed attack coordination without prior knowledge of the defense systems at the cluster head and without prior knowledge regarding other hostile nodes. Specifically, a given malicious node may not know a priori if a given neighboring node inside the network is also malicious and will participate in the attack. The framework developed in this work may serve as a starting point in the analysis of attack and defense strategies for this scenario.

# REFERENCES

[1] W. Yu, Z. Ji, and K. J. R. Liu, “Securing cooperative ad hoc networks under noise and imperfect monitoring: Strategies and game theoretic analysis,” *IEEE Transactions on Information Forensics and Security*, vol. 2, no. 2, pp. 1556–6013, June 2007.

[2] C. Hua and T.-S. P. Yum, “Asynchronous random sleeping for sensor networks,” *ACM Transactions on Sensor Networks*, vol. 3, no. 3, pp. 15–30, February 2007.

[3] T. He, S. Krishnamurthy, L. Luo, T. Yan, L. Gu, R. Stoleru, G. Zhou, Q. Cao, P. Vicaire, J. A. Stankovic, and T. F. Abdelzaher, “Vigilnet: An integrated sensor network system for energy-efficient surveillance,” *ACM Transactions on Sensor Networks*, vol. 2, no. 1, pp. 1–38, February 2006.

[4] A. Czarlinska and D. Kundur, “Reliable event-detection in wireless visual sensor networks through scalar collaboration and game theoretic consideration,” *IEEE Transactions on Multimedia, Special Issue on Multimedia Applications in Mobile/Wireless Contexts*, August 2008, to appear.

[5] C.-Y. Chong and S. P. Kumar, “Sensor networks: Evolution, opportunities and challenges,” *The Proceedings of the IEEE*, vol. 91, no. 8, pp. 1247–1256, August 2003.

[6] A. Czarlinska, W. Luh, and D. Kundur, “Attacks on sensing in hostile wireless sensor-actuator environments,” in *Proc. IEEE Globecom*, Washington, DC, November 2007, pp. 1001–1005.

[7] M. Rahimi, R. Baer, O. I. Iroezi, J. C. Garcia, J. Warrior, D. Estrin, and M. Srivastava, “Cyclops: In situ image sensing and interpretation in wireless sensor

networks," in *Proc. ACM International Conference on Embedded Networked Sensor Systems*, San Diego, CA, November 2005, pp. 192–204.

[8] A. Czarlinska, W.Luh, and D. Kundur, "G-E-M sensor networks for mission critical surveillance in hostile environments," in *Proc. IEEE INFOCOM Workshop on Mission Critical Networks*, Phoenix, AZ, April 2008, pp. 1–6.

[9] W. Luh and D. Kundur, "Distributed privacy for visual sensor networks via Markov shares," in *Proc. IEEE Workshop on Dependability and Security in Sensor Networks and Systems*, Columbia, MD, April 2006, pp. 23–34.

[10] D. Kundur, W. Luh, U. N. Okorafor, and T. Zourntos, "Emerging security paradigms for vision-rich sensor networks," *The Proceedings of the IEEE Special Issue on Distributed Multimedia*, vol. 96, no. 1, pp. 112–130, January 2008.

[11] W. Luh, D. Kundur, and T. Zourntos, "A novel distributed privacy paradigm for visual sensor networks based on sharing dynamical systems," *EURASIP Journal on Applied Signal Processing*, no. 1, pp. 218 – 234, January 2007.

[12] R. Wood, "Fly, robot fly," *IEEE Spectrum*, vol. 45, no. 3, pp. 25–29, March 2008.

[13] L. Girod, N. Ramanathan, J. Elson, T. Stathopoulos, M. Lukac, and D. Estrin, "Emstar: A software environment for developing and deploying heterogeneous sensor-actuator networks," *ACM Transactions on Sensor Networks*, vol. 3, no. 3, pp. 13–26, October 2007.

[14] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "A survey on sensor networks," *IEEE Communications Magazine*, vol. 40, no. 8, pp. 102–114, August 2002.

[15] E. Shi and A. Perrig, "Designing secure sensor networks," *IEEE Wireless Communications*, vol. 11, no. 6, pp. 38–43, December 2004.

[16] A. Basharat, N. Catbas, and M. Shah, "A framework for intelligent sensor network with video camera for structural health monitoring of bridges," in *Proc. IEEE International Conference on Pervasive Computing and Communications Workshop*, Pisa, Italy, March 2005, pp. 385–389.

[17] J.-F. Chamberland and V. Veeravalli, "Asymptotic results for decentralized detection in power constrained wireless sensor networks," *IEEE Journal on Selected Areas in Communications*, vol. 22, no. 6, pp. 1007–1015, August 2004.

[18] W. B. Heinzelman, A. P. Chandrakasan, and H. Balakrishnan, "An application-specific protocol architecture for wireless microsensor networks," *IEEE Transactions on Wireless Communications*, vol. 1, no. 4, pp. 660–670, October 2002.

[19] K. Liu and A. Sayeed, "Asymptotically optimal decentralized type-based detection in wireless sensor networks," in *Proc. IEEE International Conference on Acoustics, Speech, and Signal Processing*, Hong Kong, China, May 2004, pp. 873–876.

[20] J.-F. Chamberland, "Design of sensor networks for detection applications via large-deviation theory," Ph.D. dissertation, University of Illinois at Urbana-Champaign, Urbana, IL, June 2004.

[21] A. Czarlinska and D. Kundur, "Wireless image sensor networks: Event acquisition in attack-prone and uncertain environments," *Springer Multidimensional Systems and Signal Processing, Special Issue on Image and Video Processing in Wireless Sensor Networks*, 2008, submitted.

[22] C. Yu, S. Soro, G. Sharma, and W. Heinzelman, “Lifetime-distortion trade-off in image sensor networks,” in *Proc. IEEE International Conference on Image Processing*, San Antonio, TX, September 2007, pp. 129–132.

[23] K. Chakrabarty, S. S. Iyengar, H. Qi, and E. Cho, “Grid coverage for surveillance and target location in distributed sensor networks,” *IEEE Transactions on Computers*, vol. 51, no. 12, pp. 1448–1453, December 2002.

[24] K. Chakrabaty and S. Iyengar, “Sensor placement in distributed sensor networks using a coding theory framework,” in *Proc. IEEE Symposium on Information Theory*, Washington, DC, June 2001, pp. 157–158.

[25] H. Yu, J. Iyer, H. Kim, E. J. Kim, K. H. Yum, and P. S. Mah, “K-coverage in the presence of mobility in wireless sensor networks,” in *Proc. IEEE GLOBECOM*, San Francisco, CA, November 2006, pp. 1–5.

[26] L. Benyuan and D. Towsley, “A study of the coverage of large-scale sensor networks,” in *Proc. IEEE Mobile and Ad Hoc Systems*, Fort Lauderdale, FL, October 2004, pp. 475– 483.

[27] Y. Zou and K. Chakrabaty, “Uncertainty-aware and coverage-oriented deployment for sensor networks,” *Journal of Parallel and Distributed Computing*, vol. 64, no. 7, pp. 788–798, July 2004.

[28] S. Meguerdichian, F. Koushanfar, G. Qu, and M. Potkonjak, “Exposure in wireless ad hoc sensor networks,” in *Proc. Annual International Conference on Mobile Computing and Networking*, Rome, Italy, July 2001, pp. 139–150.

[29] H. Kim, “Topology management protocols in ad hoc wireless sensor networks,” Ph.D. dissertation, Texas A&M University, College Station, TX, December

2007.

[30] S. Capkun and J.-P. Hubaux, “Secure positioning of wireless devices with application to sensor networks,” in *Proc. IEEE INFOCOM*, Miami, FL, March 2005, pp. 1917–1928.

[31] D. Raymond and S. Midkiff, “Denial-of-service in wireless sensor networks: Attacks and defenses,” *IEEE Pervasive Computing*, vol. 7, no. 1, pp. 74–81, January 2008.

[32] A. D. Wood and J. A. Stankovic, “Denial of service in sensor networks,” *IEEE Computer*, vol. 35, no. 10, pp. 54–62, October 2002.

[33] J. McCune, E. Shi, A. Perrig, and M. K. Reiter, “Detection of denial-of-message attacks on sensor network broadcasts,” in *Proc. IEEE Symposium on Security and Privacy*, Oakland, CA, May 2005, pp. 64–78.

[34] M. Lee, E. J. Kim, and C. W. Lee, “Source identification scheme against DDoS attacks in cluster interconnects,” in *Proc. International Workshop on Network Design and Architecture*, Montreal, Quebec, August 2004, pp. 354–362.

[35] A. Czarlinska and D. Kundur, “Distributed actuation attacks in wireless sensor networks: Implications and countermeasures,” in *Proc. IEEE Workshop on Dependability and Security in Sensor Networks and Systems*, Baltimore, MD, 2006, pp. 3–12.

[36] ——, “Towards characterizing the effectiveness of random mobility against actuation attacks,” *Computer Communications Special Issue on Sensor and Actuator Networks*, vol. 30, no. 13, pp. 2546–2559, September 2007.

[37] R. Viswanathan and P. Varshney, “Distributed detection with multiple sensors: Part I - fundamentals,” *The Proceedings of the IEEE*, vol. 85, no. 1, pp. 54–63, June 1997.

[38] R. Blum, A. S. Kassam, and H. V. Poor, “Distributed detection with multiple sensors: Part II - advanced topics,” *The Proceedings of the IEEE*, vol. 85, no. 1, pp. 64–79, June 1997.

[39] A. D‘Costa and A. M. Sayeed, “Data versus decision fusion in wireless sensor networks,” in *Proc. IEEE International Conference on Acoustic, Speech and Signal Processing*, Hong Kong, China, April 2003, pp. 832–835.

[40] M. J. Osborne and A. Rubinstein, *A Course in Game Theory.* Cambridge, MA: MIT Press, 1994.

[41] L. Zhou and Z. J. Haas, “Securing ad hoc networks,” *IEEE Network*, vol. 13, no. 6, pp. 24–30, November 1999.

[42] L. Eschenauer and V. D. Gligor, “A key-management scheme for distributed sensor networks,” in *Proc. ACM Conference on Computer and Communications Security*, Washingtion, DC, November 2002, pp. 41–47.

[43] L. Buttyàn and J.-P. Hubaux, “Report on a working session on security in wireless ad hoc networks,” in *Proc. ACM Mobile Computing and Communications Review*, New York, NY, November 2002, pp. 1–17.

[44] B. Przydatek, D. Song, and A. Perrig, “SIA: Secure information aggregation in sensor networks,” in *Proc. ACM International Conference on Embedded Networked Sensor Systems*, Los Angeles, CA, November 2003, pp. 255–265.

[45] H. Chan, A. Perrig, and D. Song, “Random key predistribution schemes for sensor networks,” in *Proc. IEEE Symposium on Security and Privacy*, Oakland, CA, May 2003, pp. 197–213.

[46] M. Ramkumar and N. Memon, “On the security of random key pre-distribution schemes,” in *Proc. IEEE Workshop on Information Assurance and Security*, West Point, New York, June 2004, pp. 5–10.

[47] H. Chan, A. Perrig, and D. Song, “Wireless sensor networks,” in *Proc. Kluwer Key Distribution Techniques for Sensor Networks*, New York, NY, January 2004, pp. 277–303.

[48] A. Czarlinska, W. Luh, and D. Kundur, “On privacy and security in distributed visual sensor networks,” in *Proc. IEEE International Conference on Image Processing*, San Diego, CA, October 2008, to appear.

[49] A. Czarlinska and D. Kundur, “Reliable scalar-visual event-detection in wireless visual sensor networks,” in *Proc. IEEE Consumer Communications & Networking Conference Special Session on Image/Video Processing & Wireless Sensor Networks*, Las Vegas, NV, January 2008, pp. 660–664.

[50] ——, “Attack vs. failure detection in event-driven wireless visual sensor networks,” in *Proc. ACM Multimedia and Security Workshop*, Dallas, TX, September 2007, pp. 215–220.

[51] ——, “Event-driven visual sensor networks: Issues in reliability,” in *Proc. IEEE Workshop on Video/Image Sensor Networks*, Boulder, CO, January 2008, pp. 1–5.

[52] M. J. Osborne, *An Introduction to Game Theory.* New York, NY: Oxford University Press, 2003.

[53] J. Huang, “Wireless resource allocation: Auctions, games and optimization,” Ph.D. dissertation, Northwestern University, Evanston, IL, December 2005.

[54] R. Johari, “Efficienty loss in market mechanisms for resource allocation,” Ph.D. dissertation, M.I.T., Cambridge, MA, June 2004.

[55] S. Boyd and L. Vandenberghe, *Convex Optimization.* New York, NY: Cambridge University Press, 2004.

[56] M. Osborne and A. Rubinstein, *A Course in Game Theory.* Cambridge, MA: M.I.T Press, 1994.

[57] G. Romp, *Game Theory. Introduction and Applications.* New York, NY: Oxford University Press, 1993.

[58] R. Kannan, S. Ray, S. Sarangi, and S. Iyengar, “Minimal sensor integrity: Measuring the vulnerability of sensor grids,” *Information Processing Letters*, vol. 86, no. 1, pp. 49–55, April 2003.

[59] D. Mukhopadhyay and S. Roy, “A game based model of security for key predistribution schemes in wireless sensor network,” in *Proc. International Conference on Distributed Computing and Internet Technology*, Bhubaneswar, India, December 2005, pp. 334–347.

[60] C. Cetinkaya and M. Yildirim, “A game theoretical approach to medium access control protocol for sensor networks,” in *Proc. IIE Annual Conference and Exhibition*, Manchester, England, March 2004, pp. 161–162.

[61] P. Nurmi, "Modelling routing in wireless ad hoc networks with dynamic Bayesian games," in *Proc. IEEE Communications Society Conference on Sensor and Ad Hoc Communications and Networks*, Reston, VA, September 2004, pp. 63–70.

[62] R. Kannan, S. Sarangi, L. Ray, and S. Iyengar, "Sensor-centric quality of routing in sensor networks," in *Proc. IEEE INFOCOM*, San Francisco, CA, April 2003, pp. 692–701.

[63] T. Wang, Y. Han, P. Varshney, and P. Chen, "Distributed fault-tolerant classification in wireless sensor networks," *IEEE Journal on Selected Areas in Communication*, vol. 23, no. 4, pp. 724–734, April 2005.

[64] L. Chitnis, A. Dobra, and S. Ranka, "Aggregation methods for large-scale sensor networks," *ACM Transactions on Sensor Networks*, vol. 4, no. 2, pp. 1–36, January 2008.

[65] H. Gupta, V. Navda, S. Das, and V. Chowdhary, "Efficient gathering of correlated data in sensor networks," *ACM Transactions on Sensor Networks*, vol. 4, no. 1, pp. 1–31, March 2008.

[66] S. Yoon and C. Shahabi, "The clustered aggregation (CAG) technique leveraging spatial and temporal correlations in wireless sensor networks," *ACM Transactions on Sensor Networks*, vol. 3, no. 1, pp. 30–43, May 2007.

[67] D. Estrin, R. Govindan, J. Heidemann, and S. Kumar, "Next century challenges: Scalable coordination in sensor networks," in *Proc. ACM/IEEE International Conference on Mobile Computing and Networking*, Washington, DC, August 1999, pp. 263–270.

[68] F. Ye, H. Luo, S. Lu, and L. Zhang, “Statistical en-route detection and filtering of injected false data in sensor networks,” in *Proc. IEEE INFOCOM*, Hong Kong, China, March 2004, pp. 2446 –2457.

[69] S. Zhu, S. Setia, S. Jajodia, and P. Ning, “Interleaved hop-by-hop authentication against false data injection attacks in sensor networks,” *ACM Transactions on Sensor Networks*, vol. 3, no. 3, pp. 1–14, December 2007.

[70] S. Zhu, S. Setia, and S. Jajodia, “Leap+: Efficient security mechanisms for large-scale distributed sensor networks,” *ACM Transactions on Sensor Networks*, vol. 2, no. 4, pp. 500–528, April 2006.

[71] S. Madden, M. J. Franklin, J. M. Hellerstein, and W. Hong, “Tag: A tiny aggregation service for ad-hoc sensor networks,” in *Proc. Symposium on Operating Systems Design and Implementation*, vol. 36, Boston, MA, December 2002, pp. 131–146.

[72] N. Shrivastava, C. Buragohain, D. Agrawal, and S. Suri, “Medians and beyond: New aggregation techniques for sensor networks,” in *Proc. ACM International Conference on Embedded Networked Sensor Systems*, Baltimore, MD, November 2004, pp. 239–249.

[73] D. Wagner, “Resilient aggregation in sensor networks,” in *Proc. ACM Workshop on Security of Ad Hoc and Sensor Networks*, Washington, DC, October 2004, pp. 78–87.

[74] L. Hu and D. Evans, “Secure aggregation for wireless networks,” in *Proc. Symposium on Applications and the Internet Workshops*, Orlando, FL, January 2003, pp. 384 – 391.

[75] H. Chan, D. Song, and A. Perrig, "Secure hierarchical in-network aggregation in sensor networks," in *Proc. ACM Conference on Computer and Communication Security*, Alexandria, VA, October 2006, pp. 278–287.

[76] R. Anderson and M. Kuhn, "Tamper resistance - A cautionary note," in *Proc. USENIX Workshop on Electronic Commerce*, Oakland, CA, November 1996, pp. 3–13.

[77] ——, "Low cost attacks on tamper resistant devices," in *Proc. International Workshop on Security Protocols*, Paris, France, April 1997, pp. 125–136.

[78] O. Komerling and M. G. Kuhn, "Design principles for tamper-resistant smartcard processors," in *Proc. USENIX Workshop on Smartcard Technology*, Chicago, IL, March 1999, pp. 1–13.

[79] N. Sastry, U. Shankar, and D. Wagner, "Secure verification of location claims," in *Proc. ACM Wireless Security Workshop*, San Diego, CA, September 2003, pp. 1–10.

[80] L. Hu and D. Evans, "Using directional antennas to prevent wormhole attacks," in *Proc. Annual Network and Distributed System Security Symposium*, San Diego, CA, February 2004, pp. 2–12.

[81] X. Wang, W. Gu, S. Chellappan, K. Schoseck, and D. Xuan, "Lifetime optimization of sensor networks under physical attacks," in *Proc. IEEE Internationl Conference on Communications*, Seoul, South Korea, May 2005, pp. 3295–3301.

[82] P. Ning, A. Liu, and W. Du, "Mitigating DoS attacks against broadcast authentication in wireless sensor networks," *ACM Transactions on Sensor Networks*, vol. 4, no. 1, pp. 1–35, March 2008.

[83] A. Agah, S. K. Das, and K. Basu, "A game theory based approach for security in wireless sensor networks," in *Proc. IEEE International Conference on Performance, Computing and Communications*, Phoenix, AZ, April 2004, pp. 259–263.

[84] K. B. A. Agah and S. K. Das, "Preventing DoS attack in sensor networks: A game theoretic approach," in *Proc. IEEE International Conference on Communications*, Seoul, South Korea, May 2005, pp. 3218–3222.

[85] Z. Yan, P. Zhang, and T. Virtanen, "Trust evaluation based security solution in ad hoc networks," in *Proc. of the Nordic Workshop on Secure IT Systems*, Gjovik, Norway, October 2003, pp. 121–125.

[86] K. Ren, T. Li, Z. Wan, F. Bao, R. H. Deng, and K. Kim, "Highly reliable trust establishment scheme in ad hoc networks," *International Journal of Computer and Telecommunications Networking*, vol. 45, no. 6, pp. 687–699, August 2004.

[87] S. Ganeriwal and M. Srivastava, "Reputation-based framework for high integrity sensor networks," in *Proc. ACM Workshop on Security of Ad Hoc and Sensor Networks*, Washington, DC, October 2004, pp. 66–77.

[88] L. Lamport, R. Shostak, and M. Pease, "The Byzantine Generals' problem," *ACM Transactions on Programming Languages and Systems*, vol. 4, no. 3, pp. 382–401, July 1982.

[89] V. Kulatliumani, A. Arora, Y. Kim, P. Shankar, and R. Yedavalli, "Reliable control system design despite Byzantine actuators," in *Proc. IEEE International Parallel and Distributed Processing Symposium*, Denver, CO, April 2005, pp. 2297–2304.

[90] D. Huang and D. Medhi, “A Byzantine resilient multi-path key establishment scheme and its robustness analysis for sensor networks,” in *Proc. IEEE International Parallel and Distributed Processing Symposium*, Denver, CO, April 2005, pp. 8–16.

[91] D. Angluin, M. Fischer, and H. Jiang, “Stabilizing consensus in mobile networks,” in *Proc. IEEE Distributed Computing in Sensor Systems*, San Francisco, CA, June 2006, pp. 37–50.

[92] I. Akyildiz, T. Melodia, and K. Chowdhury, “A survey on wireless multimedia sensor networks,” *Computer Networks*, vol. 51, no. 4, pp. 921–960, March 2007.

[93] R. J. McEliece, R. B. Ash, and C. Ash, *Introduction to Discrete Mathematics.* New York, NY: Random House Inc., 1989.

[94] C. E. Shannon, “Communication theory of secrecy systems,” *Bell System Technical Journal*, vol. 28, no. 4, pp. 656–715, 1949.

[95] S. Boyd and C. Barratt, *Linear Controller Design: Limits of Performance.* Saddle River, NJ: Prentice-Hall, 1991.

[96] H. L. Van Trees, *Detection, Estimation, and Modulation Theory Part I.* New York, NY: John Wiley & Sons, Inc., 2001.

[97] A. Czarlinska and D. Kundur, “Coordination and selfishness in attacks on visual sensor networks,” in *Proc. IEEE Wireless Communications and Networking Conference*, Las Vegas, NV, March 2008, pp. 2391–2396.

[98] F. Fu and M. V. D. Schaar, “Noncollaborative resource management for wireless multimedia applications using mechanism design,” *IEEE Transactions on Multimedia*, vol. 9, no. 4, pp. 851–868, June 2007.

[99] Z. He and D. Wu, "Resource allocation and performance analysis of wireless video sensors," *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 16, no. 5, pp. 590–599, May 2006.

[100] I. Akyildiz and I. Kasimoglu, "Wireless sensor and actor networks: Research challenges," *Ad Hoc Networks Journal*, vol. 2, no. 4, pp. 3351–3677, 2004.

[101] H. Ma and Y. Liu, "Correlation based video processing in video sensor networks," in *Proc. IEEE International Conference on Wireless Networks, Communications and Mobile Computing*, Montreal, Canada, June 2005, pp. 987–992.

[102] K. Veeraraghavan, D. Peng, and H. Sharif, "Energy efficient multi-resolution visual surveillance on wireless sensor networks," in *Proc. IEEE International Conference on Electro Information Technology*, Lincoln, NE, May 2005, pp. 6–12.

[103] D. Maniezzo, K. Yao, and G. Mazzini, "Energetic trade-off between computing and communication resource in multimedia surveillance sensor network," in *Proc. IEEE Conference on Mobile and Wireless Communications Networks*, Stockholm, Sweden, September 2002, pp. 373–376.

[104] C. Margi, V. Petkov, K. Obraczka, and R. Manduchi, "Characterizing energy consumption in a visual sensor network testbed," in *Proc. IEEE International Conference on Testbeds and Research Infrastructures for the Development of Networks and Communities*, Barcelona, Spain, March 2006, pp. 1–8.

[105] T. Aach and A. Kaup, "Statistical model-based change detection in moving video," *Signal Processing*, vol. 31, no. 1, pp. 165–180, March 1993.

[106] L. Hongliang, L. Guizhong, Z. Zhongwei, and L. Yongli, “Adaptive scene-detection algorithm for VBR video stream,” *IEEE Transactions on Multimedia*, vol. 6, no. 4, pp. 624–633, August 2004.

[107] M. Eltoweissy, M. Moharrum, and R. Mukkamala, “Dynamic key management in sensor networks,” *IEEE Communications Magazine*, vol. 44, no. 4, pp. 122–130, April 2006.

[108] M. Eltoweissy, A. Wadaa, S. Olariu, and L. Wilson, “Scalable cryptographic key management in wireless sensor networks,” *Journal of Ad Hoc Networks Special issue on Data Communications and Topology Control in Ad Hoc Networks*, vol. 3, no. 5, pp. 796–802, September 2005.

[109] H. Chan, A. Perrig, and D. Song, “Random key predistribution schemes for sensor networks,” in *Proc. IEEE Symposium on Security and Privacy*, Oakland, CA, May 2003, pp. 197–213.

[110] K.-Y. Chow, K.-S. Lui, and E. Lam, “Efficient on-demand image transmission in visual sensor networks,” *EURASIP Journal on Advances in Signal Processing*, vol. 2007, no. 5, pp. 323–333, February 2007.

[111] ——, “Balancing image quality and energy consumption in visual sensor networks,” in *Proc. IEEE International Symposium on Wireless Pervasive Computing*, Phuket, Thailand, January 2006, pp. 201–205.

[112] V. Rodriguez, “Resource management for scalably encoded information: the case of image transmission over wireless networks,” in *Proc. IEEE International Conference on Multimedia and Expo*, Baltimore, MD, July 2003, pp. 813–816.

[113] S. Bandyopadhyay and E. Coyle, “An energy efficient hierarchical clustering

algorithm for wireless sensor networks," in *Proc. IEEE INFOCOM*, San Francisco, CA, March 2003, pp. 1713–1723.

[114] S. Olariu, M. Eltoweissy, and M. Younis, "ANSWER: Autonomous networked sensor system," *Journal of Parallel and Distributed Computing*, vol. 67, no. 1, pp. 111–124, January 2007.

[115] P. L. Rosin, "Thresholding for change detection," *Computer Vision and Image Understanding*, vol. 86, no. 2, pp. 79–95, May 2002.

[116] M. Wu and C. Chen, "Collaborative image coding and transmission over wireless sensor networks," *EURASIP Journal on Advances in Signal Processing*, vol. 1, no. 70481, pp. 1–9, January 2007.

[117] R. Radke, S. A. O. Al-Kofahi, and B. Roysam, "Image change detection algorithms: A systematic survey," *IEEE Transactions on Image Processing*, vol. 14, no. 3, pp. 294–307, March 2005.

[118] T. Aach and A. Kaup, "Bayesian algorithms for adaptive change detection in image sequences using Markov random fields," *Signal Processing Image Communication*, vol. 1, no. 2, pp. 147–160, August 1995.

[119] K. V. Mardia and I. L. Dryden, "The statistical analysis of shape data," *Biometrika*, vol. 76, no. 1, pp. 271–281, January 1989.

[120] S. Ganeriwal, A. Kansal, and M. Srivastava, "Self aware actuation for fault repair in sensor networks," in *Proc. IEEE International Conference on Robotics and Automation*, vol. 5, Barcelona, Spain, April 2004, pp. 5244–5249.

[121] M. Rahimi, H. Shah, G. S. Sukhatme, J. Heideman, and D. Estrin, "Studying the feasibility of energy harvesting in a mobile sensor network," in *Proc.*

*IEEE International Conference on Robotics and Automation*, Taipei, Taiwan, September 2003, pp. 19–24.

[122] S. Čapkun, J.-P. Hubaux, and L. Buttyàn, "Mobility helps security in ad hoc networks," in *Proc. ACM International Symposium on Mobile Ad Hoc Network and Computing*, Annapolis, MD, June 2003, pp. 46–56.

[123] M. Laibowitz and J. Paradiso, "Parasitic mobility in dynamically distributed sensor networks," in *Proc. International Conference on Pervasive Computing*, vol. 3468, Munich, Germany, May 2005, pp. 255–278.

[124] S. Meguerdichian, F. Koushanfar, M. PotKonjak, and M. B. Srivastava, "Coverage problems in wireless ad-hoc sensor networks," in *Proc. IEEE Infocom*, Anchorage, AK, April 2001, pp. 1380–1387.

[125] ——, "Worst and best-case coverage in sensor networks," *IEEE Transactions on Mobile Computing*, vol. 4, no. 1, pp. 84–92, January 2005.

[126] X. Li, Peng-JunWan, and O. Frieder, "Coverage in wireless ad hoc sensor networks," *IEEE Transactions on Computers*, vol. 52, no. 6, pp. 753–763, June 2003.

[127] D. Mehta, M. Lopez, and L. Lino, "Optimal coverage paths in ad-hoc sensor networks," in *IEEE International Conference on Communications*, Anchorage, AK, May 2003, pp. 507–511.

[128] J. Liu, X. Koutsoukos, J. Reich, and F. Zhao, "Sensing field: Coverage characterization in distributed sensor networks," in *Proc. IEEE International Conference on Acoustics, Speech, and Signal Processing*, Hong Kong, China, April 2003, pp. 173–176.

[129] G. Kesidis, T. Konstantopoulos, and S. Phoha, "Surveillance coverage of sensor networks under a random mobility strategy," in *Proc. IEEE Sensors*, Toronto, Canada, October 2003, pp. 961–965.

[130] R. Kannan, S. Sarangi, S. Ray, and S. S. Iyengar, "Minimal sensor integrity: Measuring the vulnerability of sensor deployments," *Information Processing Letters*, vol. 86, no. 1, pp. 49–55, April 2003.

[131] S. Meguerdichian, S. Slijepcevic, V. Karayan, and M. Potkonjak, "Localized algorithms in wireless ad-hoc networks: Location discovery and sensor exposure," in *Proc. ACM International Symposium on Mobile Ad Hoc Networking and Computing*, Long Beach, CA, October 2001, pp. 106–116.

[132] A. Tews, M. J. Mataric, and G. Sukhatme, "Avoiding detection in a dynamic environment," in *Proc. IEEE International Conference on Intelligent Robots and Systems*, Sendai, Japan, September 2004, pp. 3773–3778.

[133] A. Howard, J. J. Matarić, and G. S. Sukhatme, "An incremental self-deployment algorithm for mobile sensor networks," *Autonomous Robots Special Issue on Intelligent Embedded Systems*, vol. 13, no. 2, pp. 113–126, September 2002.

[134] W. Xu, W. Trappe, Y. Zhang, and T. Wood, "The feasibility of launching and detecting jamming attacks in wireless networks," in *Proc. ACM International Symposium on Mobile Ad Hoc Networking and Computing*, Urbana, IL, May 2005, pp. 46–57.

[135] K. Ma, Y. Zhang, and W. Trappe, "Mobile network management and robust spatial retreats via network dynamics," in *Proc. IEEE International Conference on Mobile Ad Hoc and Sensor Systems*, Washington, DC, November 2005, pp. 202–209.

[136] A. Wood, J. Stankovic, and S. Son, “Jam: A jammed-area mapping service for sensor networks,” in *Proc. IEEE International Real-Time Systems Symposium*, Cancun, Mexico, December 2003, pp. 286–297.

# APPENDIX A

# STEALTHY DIRECT ATTACK ANALYSIS

## 1. Non-negativity of Terms Outside Log in Proof of Theorem 2

The terms with $q$ solely in the exponent can never be negative. The term $(1-q)^{n(1-q)} > 0$ since $q \leq 1$. Now suppose that $2p = \min\{2p, 2(1-p)\}$, which implies $p \leq 1/2$. Then $1-p-q/2 \geq 1-2p \geq 0$ since $p \leq 1/2$, and $p-q/2 \geq 0$ since $q \leq 2p$. On the other hand, supposed that $2(1-p) = \min\{2p, 2(1-p)\}$, which implies $p \geq 1/2$. Then $1-p-q/2 \geq 0$ since $q \leq 2(1-p)$, and $p-q/2 \geq 2p-1 \geq 0$ since $p \geq 1/2$.

## 2. Non-positivity of Log Term in Proof of Theorem 2

We show that the argument inside ln, $\alpha(q) = (4(p-q/2)(1-p-q/2))/((1-q)^2) \leq 1$, in the well-defined interval, hence showing that the ln term is always non-positive.

$$\frac{\partial \alpha(q)}{\partial q} = -\frac{2(1-2p)^2}{(1-q)^3} \tag{A.1}$$

Eq. (A.1) is always non-positive, so $\alpha(q)$ is monotonically decreasing. The largest value $\alpha(q)$ takes is at $q = 0$, and this value is $4p(1-p) \leq 1$ since $p = 0.5$ yields the maximum value of 1.

## 3. Uncoordinated Attack Analysis

In this appendix we discuss the background analysis for the uncoordinated stealthy direct attack game. A methodology for determining the Nash equilibria of a game is via the best response function shown in Eq. (A.2).

$$B_i(a_{-i}) = \{a_i \in A_i : u_i(a_i, a_{-i}) \geq u_i(a_i', a_{-i})\} \qquad \text{(A.2)}$$
$$for \quad all \quad a_i' \in A_i$$

The action profile $a^*$ is a Nash equilibrium of a strategic game *iff* every player's action is a best response to the other players' actions, that is, $a_i^* \in B_i(a_{-i}^*)$ for every player $i$. For the case of an uncoordinated stealthy direct game we obtain the following best response functions.

$$B_i(q_j) = 0 \quad if \quad q_j \leq T_p \qquad \text{(A.3)}$$
$$B_i(q_j) = 1 \quad if \quad q_j \geq T_p$$
$$T_p = 1/\beta_p \qquad \text{(A.4)}$$
$$\beta_p \in [1, 1.5]$$

Via the intersection of the two best response functions, there are two Nash equilibria given by:

$$(q_{1,N}, q_{2,N}) = \{(0,0), (1,1)\} \qquad \text{(A.5)}$$

The utilities achievable at these Nash equilibria are given by:

$$\pi_i(0,0) = 1 \qquad \text{(A.6)}$$
$$\pi_i(1,1) = \beta_p - 1 \qquad \text{(A.7)}$$

**Proof 13**

$$\frac{\partial \pi_i(q_1, q_2)}{\partial q_i} = \beta_p q_j - 1 \qquad \text{(A.8)}$$
$$q_j = \frac{1}{\beta_p}$$

*Thus* $(q_i, q_j) = (1/\beta_p, 1/\beta_p)$ *is a point of interest since we note that both players are* indifferent *among the set of actions available to them. Specifically, all actions* $q_i \in [0,1]$ *result in the same utility which is independent of that action and depends only on the value of* $\beta_p$*. By examining Figure 23, we see that this point corresponds to the saddle point of the manifold. As we will show, this point represents an important threshold that influences a node's optimal response.*

$$\begin{aligned}\pi_1(q_1, \frac{1}{\beta_p}) \quad &= 1 + \beta_p(\tfrac{1}{\beta_p})q_1 - \tfrac{1}{\beta_p} - q_1 \\ &= 1 - \tfrac{1}{\beta_p} \\ &= \pi_1(\tfrac{1}{\beta_p}) \end{aligned} \tag{A.9}$$

*To understand what happens away from this point, we examine the utility* $\pi_1$ *for a fixed* $p$ *and* $q_2$*. Let* $\tilde{q}_2 = 1/\beta_p + \epsilon$ *where* $\epsilon > 0$*. Then:*

$$\begin{aligned}\pi_1(q_1, \tilde{q}_2) &= 1 + \beta_p(\frac{1}{\beta_p} + \epsilon)q_1 - q_1 - (\frac{1}{\beta_p} + \epsilon) \\ &= 1 - (\frac{1}{\beta_p} + \epsilon) + (\beta_p\epsilon)q_1 \end{aligned} \tag{A.10}$$

*It is easy to see that for any* $\hat{q}_1 > q_1$*,* $\pi_1(\hat{q}_1) > \pi_1(q_1)$ *since* $\beta_p \in [1, 1.5]$ *and* $\epsilon > 0$*. Thus the function is strictly increasing in* $q_1$ *with the maximum occurring at the edge of the interval* $[0,1]$*, namely at* $q_1 = 1$*, yielding the utility* $\pi_1(q_1 = 1) = 1 - (1/\beta_p + \epsilon) + \beta_p\epsilon$*. Therefore we conclude that* $B_1(q_2) = 1$ iff $q_2 > 1/\beta_p$*.*

*In summary, the best response of* $q_1$ *to* $\tilde{q}_2 = 1/\beta_p + \epsilon$ *for* $\epsilon > 0$ *is to actuate with* $q_1 = 1$*. Now we consider the next iteration and we determine the best response of* $\tilde{q}_2$ *to* $q_1 = 1$*. Node 2's utility is given by:*

$$\begin{aligned}\pi_2(q_1, q_2) &= 1 - (q_1 + q_2) + \beta_p q_1 q_2 \\ \pi_2(1, \tilde{q}_2) &= \tilde{q}_2(\beta_p - 1) \end{aligned} \tag{A.11}$$

*The maximum of this function is achieved by setting $\tilde{q}_2 = 1$, giving a maximal utility of $\pi_i(1,1) = \beta_p - 1$. Thus the pure Nash equilibrium is given by:*

$$(q_{1,N}, q_{2,N}) = (1,1) \tag{A.12}$$

$$u_i(1,1) = \beta_p - 1 \tag{A.13}$$

*Similarly if we let $\tilde{q}_2 = 1/\beta_p - \epsilon$ where $\epsilon > 0$. Then:*

$$\begin{aligned}\pi_1(q_1, \tilde{q}_2) &= 1 + \beta_p(\frac{1}{\beta_p} - \epsilon)q_1 - q_1 - (\frac{1}{\beta_p} - \epsilon)\\ &= 1 - (\beta_p\epsilon)q_1 - (\frac{1}{\beta_p} - \epsilon)\end{aligned} \tag{A.14}$$

*This function is strictly decreasing with $q_1$ since $\beta_p \in [1, 1.5]$ and since $\epsilon > 0$ with the minimum occurring at the left end point of the interval $[0,1]$, namely at $q_1 = 0$. This results in the maximum utility $\pi_1(q_1 = 0) = 1 - (1/\beta_p - \epsilon)$.*

*Therefore we have determined that the best response of $q_1$ to $q_2 = (1/\beta_p) - \epsilon$ for $\epsilon > 0$ is to set $q_1 = 0$. We now iterate the best response procedure to find the optimal response of $q_2$ to $q_1 = 0$. The utility of node 2 $\pi_2$ is given by:*

$$\begin{aligned}\pi_2(q_1, q_2) = \pi_2(q_1, q_2) &= 1 - (q_1 + q_2) + \beta_p q_1 q_2\\ \pi_2(0, \tilde{q}_2) &= 1 - q_2\end{aligned} \tag{A.15}$$

*This utility is maximized by choosing $q_2 = 0$. Therefore $(q_{1,N}, q_{2,N}) = (0,0)$ is another equilibrium point of the game and yield the utility $\pi_i = 1$ to each of the players.*

*In summary we conclude that $B_i(q_j) = 0$ iff $q_j < 1/\beta_p$ and that $B_i(q_j) = 1$ iff $q_j > 1/\beta_p$.*

# APPENDIX B

# STEALTHY IMAGE SENSOR NETWORK ANALYSIS

In this appendix we analyze in greater detail the statistics of a representative image sequence, that is Seq. 2 from Figure 45, showing a moving car with trees. As pointed out in Aach and Kaup [105], [118], the difference pixels $D_i$ generally do not obey a normal distribution model though this assumption is commonly made. To investigate the possible distribution of the difference pixels, we make use of a typical q-q plot as shown in Figure 57 for the moving car sequence.

The q-q plot is used to test whether a set of samples are empirically Gaussian. The Gaussian assumption is rejected if the q-q plot returns a set of points that lie far off the straight line. As shown in Figures. 57a and 57b, this is indeed the case for the car sequence under both hypotheses. The points lying off the main line may either indicate the presence of massive outliers in the data (the difference pixels), or may indicate that the distribution is not Gaussian. We thus call upon the use of histograms to provide further clues regarding the pixel distribution. The histograms for the difference images under the two hypotheses are shown in Figure 58a and 58b.

These histograms show that the distributions are most likely bell-shaped as can be confirmed through the use of Mardia statistics [119]. Based on the q-q plots and the histograms, we thus approximate the difference pixels as Gaussian. We note however that this assumption tends to fail for event frames (alternative hypothesis) where regions of interest that undergo change have a different distribution than regions of no change. Hence strictly speaking the Gaussian assumption only holds for certain non-event frames and certain regions of an event frame. It is nevertheless a helpful approximation that leads to a non-parametric (robust) detector.

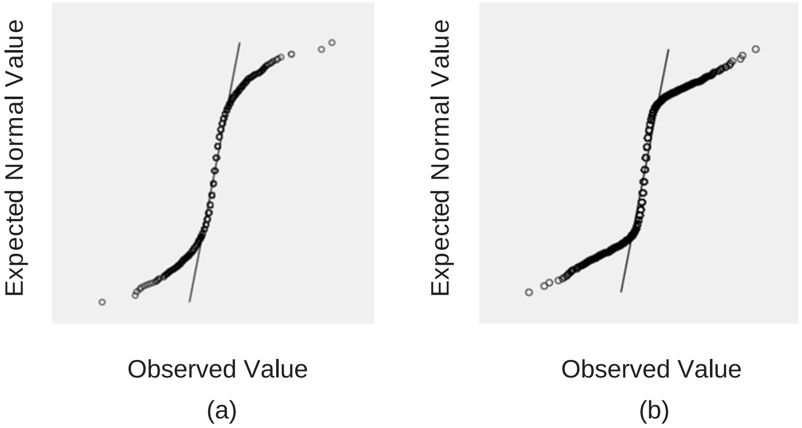


Fig. 57. Test for normality of difference images or q-q plot (car sequence) under ($a$) $\mathcal{H}_0$. ($b$) $\mathcal{H}_1$.

In addition to the distribution assumption, we also consider the assumption that $\sigma_1^2 > \sigma_0^2$. Indeed this assumption is imperfect since in order for every difference pixel in an event frame to have $\sigma_1^2$, the object would have to move across the *entire* frame, thus covering all pixels. In Aach and Kaup [105], [118], smaller blocks are assumed to mitigate this flaw. However through our use of entire difference frames, this assumption does not hold. To mitigate this issue we can assume that the effect of a small movement can be distributed across all pixels by decreasing $\sigma_1^2$. This assumption is more realistic since if we use the entire frame to estimate $\sigma_1^2$, then the estimate of $\sigma_1^2$ will mostly be of the non-moving regions. Thus the variance will be decreased to $\sigma_1^2 \approx \sigma_0^2$, leading to the use of a robust (non-parametric) detector.

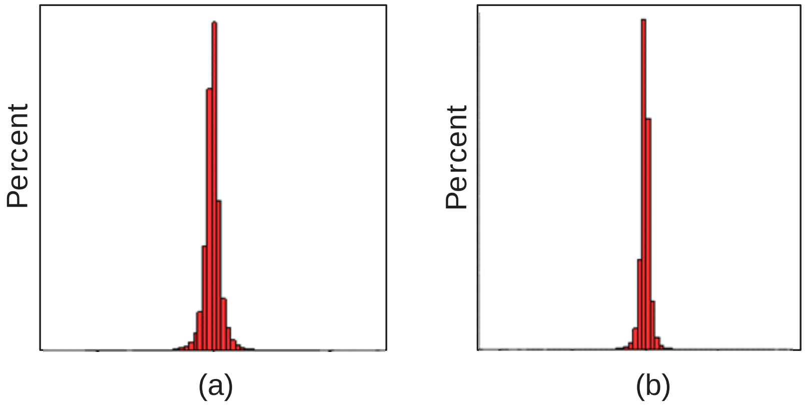


Fig. 58. Difference image histogram (car sequence) under $(a)$ $\mathcal{H}_0$. $(b)$ $\mathcal{H}_1$.

# APPENDIX C

# SENSOR AND ACTUATOR TECHNOLOGIES

The functionality and envisioned capabilities of individual sensor nodes and of sensor networks as a whole continue to broaden with advances in various micro technologies [100], [92]. Indeed sensor nodes are increasingly acquiring robot-like qualities through the addition of various actuation functionalities and robotic devices are increasingly shrinking in size to resemble nodes. For instance, tiny flying robots the size of a penny (3 centimeters wingspan and weighting 60 milligrams not including the battery [12]) are envisioned for remote aerial surveillance and data acquisition. Other robotic/sensor-like devices are being tested for aquatic environments and land applications.

In the scope of this work, actuation in sensor networks is defined broadly as the ability of a node to act upon, change or influence its environment using limited energy. The latter requirement is in contrast with more traditional robotic actuation where the robot typically has access to a much larger battery or wired source of energy. The small size (especially height) of the node and of its components further restricts the type and range of actuation that it may perform, in contrast with much larger robots. The energy and size limitations imply that sensor nodes should employ distributed actuation to limit energy use while having a global effect on the environment.

In the context of hostile distributed sensor networks, actuation to perturb the data acquisition of nearby sensors may include magnetic, acoustic, motion-based, light-based and particle dispersion-based actuation and may include mobility to traverse a given landscape to re-shape the topology of the environment. Such actuation may be particularly detrimental to the data acquisition of binary sensors where a local decision threshold is utilized. If this threshold can be guess-estimated or captured from the sensor nodes, it may be utilized to the hostile network's advantage. For instance, based on the knowledge of such a threshold and based on its own local readings, each hostile node can determine if the neighboring sensor should report a 1 or 0 and thus actuate to effectively flip this decision. When several hostile nodes are acting upon a single sensor, they may utilize a timing protocol to ensure that each hostile node actuates in the manner that will flip the sensor's decision.

Although not the central focus of this work, other important forms of actuation in sensor networks include mobility [35], [36]. We thus briefly overview some interesting results from the sensor network mobility literature as well as from the related fields of sensor network coverage and deployment. Importantly this brief overview of a large and growing sensor network field is not intended to be exhaustive but rather illustrative. In [120] the authors explore how mobility can be used by a sensor network as a type of actuation to repair its own coverage (called self-repair). In [121] the authors examine how mobile nodes can migrate to areas of high energy (solar for example) to charge themselves and then charge other starving nodes. In [122] and [35] the authors discuss how mobility can specifically help sensor network security by detecting misbehaving nodes. In [123] the authors introduce the idea of parasitic mobility where nodes are able to catch a ride on any moving object and dislodge from it using an actuator. Hence adding actuation in the form of mobility to sensor networks significantly expands their autonomy and fault-tolerance.

The exact definition of sensor network coverage varies depending on the specific application and on the toolsets used to address it. Generally speaking however, coverage is a measure of how well the sensor network covers or observes all the points of a physically distributed phenomenon. In [124], [125], [126] and [127] the authors formulate the Best and Worst case coverage scenarios by calculating a path of Maximum Support and Maximum Breach for an object moving through the sensor field. References [128], [129], [23], [24] and [130] present other key results in coverage. In reference [26] the authors use percolation theory to study the sensor network density required to achieve detection of a target with probability 1 almost surely. In [27] the authors consider the problem of coverage in the face of uncertainty in the sensor locations. In [131] the authors provide local algorithms for location discovery and coverage. This research is critical for understanding how a hostile entity might find a path of least detection through the environment and how a hostile network might "cover" the legitimate nodes in the face of uncertainty of their locations.

In [28] the authors formulate exposure as a measure of how well an object moving on an arbitrary path can be observed by the sensor network over a period of time. The authors present an efficient algorithm for finding minimal exposure paths for the object to move along, which also simultaneously provides information about the worst case coverage of the sensor network. Simulation results show that for generally sparse fields with a random *uniform* spatial deployment, there exist many minimal exposure paths. The authors also present a generalized sensing model of interest to the study of actuation.

References [132] and [133] provide an approach that allows a stealthy traverse through an *unknown* environment that contains dynamic objects and an observer. The key is to exploit the dynamic objects in the environment as they become known and use their shadow as cover to move undetected from an initial location to a target location. The observer is assumed to have infinite observational range in all directions. The traversing robots are assumed to also have omni-directional sensing but for finite ranges. Simulations and implementation results show that 100% stealth can be achieved at a tradeoff of taking a route which is 86% efficient compared with a direct route which is 100% efficient but only 36% stealthy.

A number of pioneering works have proposed mobility as a type of active defense against the actuation attack of radio jamming. In [134] the authors study both the feasibility of launching jamming attacks and the challenges associated with detecting such attacks. Of particular interest is their observation that a single type of measurement usually does not suffice to correctly detect the attack. This correlates with our findings that without adequate side information (model of the attack or its parameters), detection is challenging and that involved protocols may not be most cost effective for the detection level they produce. In [135] the authors argue that mobility is advantageous to network operations and show how spatial escape strategies can prevent a mobile jammer from partitioning the network. Although similar in spirit to our work from [36], the proposed mobility model requires some computation and further requires that the operational goals of the network be first expressed in terms of potential functions. Mobility of nodes ensues as a result of these potential forces and the associated network dynamics. Furthermore [135] focuses on attacking nodes that are concentrated in a specific region rather than distributed throughout the entire space as in our studies. In [136] the authors propose a mapping protocol which uses loose group semantics, eager eavesdropping, supremacy of local information and robustness to packet loss to detect jammed regions in real-time. This work once again focuses exclusively on jamming attacks - specifically on a subset of highly localized attacking nodes, and requires the use of a protocol to actively detect the attack.

These works suggest that including actuation abilities in sensor networks significantly expands their functionality, autonomy and fault-tolerance. Importantly these works also suggest that at the same time, adding actuation abilities to a network that is *hostile* poses an increased challenge for security and reliable data acquisition. These observations motivate the need to study the competing sensor networks scenario for data acquisition which is the focus of this work.

# VITA

Aleksandra Czarlinska received her B.A.Sc. degree in engineering science electrical option in 2002 from the University of Toronto, Canada, where she was the recipient of the National Scholarship Award. During the course of her Ph.D. studies at Texas A&M University she served as a research assistant, teaching assistant and as a lecturer in the Department of Electrical & Computer Engineering. She is a student member of the IEEE and received the P.E.O. Scholarship Award during her Ph.D. studies. She participated in the Research Experience for Undergraduates (REU) program at Texas A&M University as a graduate assistant and mentor from 2005-2008. Her current research focuses on the identification and prevention of new security attacks in mobile wireless sensor and actuator networks and on the application of game theory to distributed systems. Aleksandra Czarlinska can be reached at 214 Zachry Engineering Center, College Station, TX 77843, Mailstop 156.

The typist for this dissertation was Aleksandra Czarlinska.