REAL-TIME PROCESSING OF A LONG PERIMETER FIBER OPTIC INTRUSION SYSTEM

A Senior Scholars Thesis

by

WILLIAM TIMOTHY SNIDER

Submitted to the Office of Undergraduate Research
Texas A&M University
in partial fulfillment of the requirements for the designation as

UNDERGRADUATE RESEARCH SCHOLAR

April 2008

Major: Electrical Engineering

REAL-TIME PROCESSING OF A LONG PERIMETER FIBER OPTIC INTRUSION SYSTEM

A Senior Scholars Thesis

by

WILLIAM TIMOTHY SNIDER

Submitted to the Office of Undergraduate Research
Texas A&M University
in partial fulfillment of the requirements for the designation as

UNDERGRADUATE RESEARCH SCHOLAR

Approved by:

Research Advisor: Christi K. Madsen
Associate Dean for Undergraduate Research: Robert C. Webb

April 2008

Major: Electrical Engineering

ABSTRACT

Real-Time Processing of a Long Perimeter Fiber Optic Intrusion System (April 2008)

William Timothy Snider
Department of Electrical and Computer Engineering
Texas A&M University

Research Advisor: Dr. Christi K. Madsen
Department of Electrical and Computer Engineering

This thesis reports on recent advances made in real-time intruder detection for an intrusion system developed at Texas A&M University that utilizes a phase-sensitive optical time-domain reflectometer. The system uses light pulses from a highly coherent laser to interrogate a length of buried optical fiber. The Rayleigh backscattered light is detected, and a FPGA-based system is used to implement real-time signal processing algorithms. With the introduction of real-time signal processing, the system can run continuously, only triggering intrusions when they are detected. These recent advances allow for more effective processing of intruder signatures, while still giving results comparable to previous off-line signal processing results. With these advances, this technology is a prime candidate for low-cost perimeter monitoring of high-value and high-security targets, such as nuclear power plants, military bases, and national borders.

ACKNOWLEDGMENTS

I would like to give special thanks to Dr. Christi Madsen for her valuable guidance. Coming into this project my knowledge of fiber optics was limited, but I have learned a great deal through research and meetings with her. I would also like to acknowledge the late Dr. Henry Taylor for his invention of the ϕ-OTDR system and his work to make it a reality. His work laid the foundation for this research project.

Portions of this research were conducted as part of the 2007 Research Experience for Undergraduates (REU) Program at Texas A&M University. Funding for this program was provided by the National Science Foundation (NSF) and Department of Defense (DoD).

NOMENCLATURE

ϕ-OTDR	Phase Sensitive Optical Time Domain Reflectometer
EM	Electromagnetic
FFT	Fast Fourier Transform
FPGA	Field Programmable Gate Array
MS/sec	Million Samples per Second
PZT	Piezoelectric Cylinder
RF	Radio Frequency

TABLE OF CONTENTS

LIST OF FIGURES

CHAPTER I

INTRODUCTION

Security systems are widely used today, with the goal of detecting unwanted intruders. These systems can range from the simple to the elaborate, but the overall philosophy is to provide "appropriate and cost-effective protection for building occupants" [1]. Traditional security systems, including seismic sensors, cameras, motion detectors, and fences, have limited range and several drawbacks. They are deployed above ground, allowing for them to be seen and giving the intruder a chance of dodging detection. Power support is also required, which could be challenging in remote locations. Long perimeters increase the number of components necessary, adding to the overall complexity of the system.

A distributed fiber optic perimeter sensor, as shown in Fig. 1, offers several advantages over traditional perimeter monitoring technologies. A single cable allows for monitoring along its length for tens of kilometers, with the possibility to extend to hundreds of kilometers through the use of fiber amplifiers. Access is only needed to one end of the fiber to place the laser and detectors. This is beneficial, because it is not necessary to backtrack the buried fiber in order to gain access to the opposite end. Additionally,

---

This thesis follows the style of *IEEE Journal of Lightwave Technology*.

intrusions can be localized to a specific point along the length of fiber. The United States-Mexico border stretches 1,952 miles, and in 2004 there were 1.1 million apprehensions along the border [2]. The range and resolution of a fiber optic sensor makes this technology a good candidate for border surveillance. On a smaller scale, this technology can be used to monitor the entire perimeter of an embassy, military base, power plant, or other high profile target.

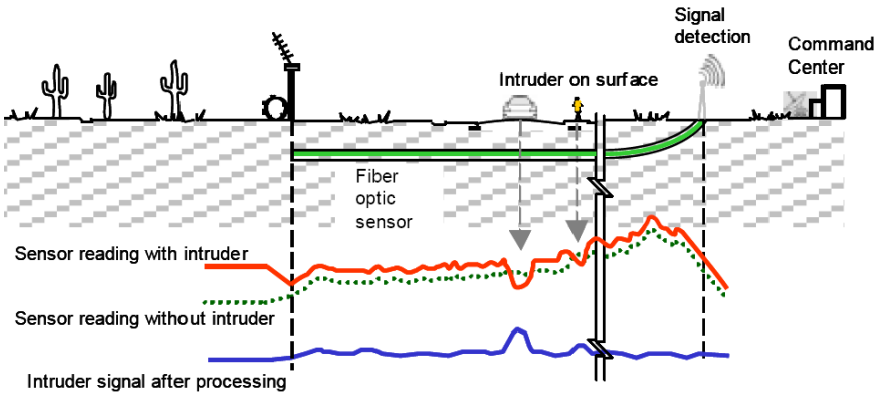

Fig. 1. Schematic for a distributed fiber optic intrusion sensor. Sketches of the backreflected signal are shown on the lower portion of the diagram.

A distributed fiber optic intrusion system consists of a buried length of optical fiber monitored from a central location. Having a buried fiber reduces the ability to tamper with the system, there is no emanation from the fiber that can be detected, and optical communication is not susceptible to electromagnetic (EM) or radio frequency (RF) interference [3]. The sensor necessary for the detection of intruders has already been developed in previous research at Texas A&M University [4]. The pressure and seismic waves of an intruder on the ground interact with the buried fiber to produce a phase

change in the backscattered light. A phase-sensitive optical time domain reflectometer (ϕ-OTDR) detects these phase changes and represents them as amplitude changes. Developed software tracks these amplitude changes over time, allowing for the realization of intrusions.

This research involved the continued development of the fiber optic intrusion sensor. In order for a security system to be practical, it must have real-time intrusion detection capabilities. Instant notification of potential intruders is necessary if they are to be stopped. For this project, a field programmable gate array (FPGA) was used to achieve real-time signal processing. In order to increase sensitivity, a highly coherent laser was also used. Field tests at Texas A&M University's Riverside Campus were conducted to determine the effectiveness of new real-time signal processing algorithms in triggering intrusions.

This thesis focuses on the development of a real-time signal processing algorithm, which brings the buried fiber optic intrusion system one step closer to real-world implementation. In the remaining chapters, the background for the development of the signal processing algorithm, the experimental procedure used for analysis, results, conclusions, and recommendations for future work will be discussed.

CHAPTER II

BACKGROUND INFORMATION

Texas A&M University received a patent on the "Apparatus and method for fiber optic intrusion sensing" in 1993 [4]. The basic foundation for an intrusion system exists, with current research focusing on making advances in real-time intruder detection. This is a key component for any intrusion system, as it does no good to receive notification of an intruder once they have already had time to escape.

Phase sensitive OTDR

The ϕ-OTDR is the backbone of this system, as it provides a means to detect the changes in backscattered light caused by an intrusion. Optical time domain reflectometers (OTDR) were first demonstrated for use in fiber optic sensing over two decades ago [5]. The ϕ-OTDR measures phase changes, as opposed to attenuation changes with the traditional OTDR, making it orders of magnitude more sensitive to perturbations along the fiber [4, 6, 7]. The block diagram for the ϕ-OTDR can be seen in Fig. 2.

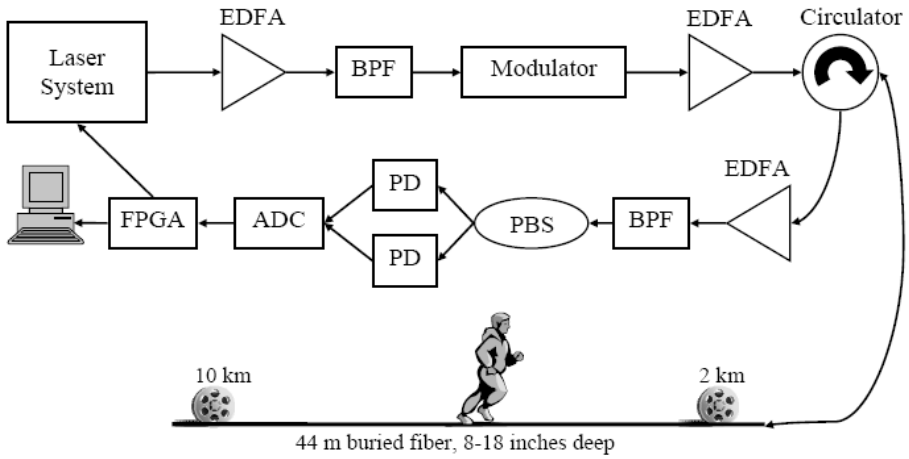

Fig. 2. Block diagram for ϕ-OTDR. EDFA=erbium doped fiber amplifier, BPF=bandpass filter, PBS=polarization beam splitter, PD=photodetector, ADC=analog-to-digital converter, and FPGA=field programmable gate array.

A highly coherent laser with a stabilized center frequency is used to introduce pulses of light into the optical fiber. A modulator is used to break the continuous output from the fiber laser into 2μs pulses of light. The pulse period is chosen to be longer than the time required for the optical pulse to propagate the length of the fiber and the Rayleigh backscattered signal to be completely detected, which is 120 μs in the test setup. By using a pulse period of 150 μs, it is ensured that there is no overlap of consecutive pulses, and therefore no overlap of data.

Fiber amplifiers are used at various points in the system to increase the power transmitted down the fiber and the power of the Rayleigh backscattered light. Since the pulse is introduced and the Rayleigh backscattered light monitored from the same end of the fiber, an optical circulator is used to separate the signals. The backscattered signal is

split into two channels using a polarization beam splitter to optimize the probability of detection [8].

Data acquisition and processing over two channels is handled by National Instrument's PCI-7831R FPGA card with LabVIEW software control. In order to connect the system outputs to the FPGA, it is necessary to use an analog-to-digital converter.

Field programmable gate array

Continuous real-time signal processing is desired in order to monitor the buried optical fiber for intrusions. Programs developed in LabVIEW running in Windows are not able to keep up with the incoming data, and within several seconds are already lagging. This is because traditional LabVIEW programs run in Windows have a maximum loop rate of 1 kHz. Using a FPGA, it is possible to run loop rates up to 40 MHz. This significant increase in speed allows for the realization of real-time signal processing algorithms.

National Instrument's LabVIEW software is widely used in industry to develop scalable test, measurement, and control applications. Previously, hardware utilizing a FPGA required understanding and using bit code to program it, which the average engineer does not know. Through the use of LabVIEW's FPGA Module, their standard graphical interface can be used to program the FPGA device, and then LabVIEW handles the compilation of the necessary bit code. This allows the average engineer to design

custom hardware for a specific task [9]. For this project, National Instrument's PCI-7831R FPGA card was used, which can be seen in Fig. 3.

Fig. 3. National Instrument's PCI-7831R FPGA card. The FPGA allows for high frequency loop rates.

One drawback with the FPGA is that it is limited to integer operations only. This limitation has a major impact on filter design. While LabVIEW provides a way to convert filters into fixed point filters, the conversion is never exact, and sometimes gives a completely different frequency response. For this project, a filter was designed with a close enough match to the desired frequency response.

Riverside test facility

Field testing was conducted at Texas A&M University's Riverside Campus, where 44 m of optical fiber are buried in clay soil at depths of 8-18 inches below the surface. A room located next to the buried cable contains the laser and detection equipment, with

the fiber passing through conduits in the wall. The fiber layout at the Riverside test facility can be seen in Fig. 4.

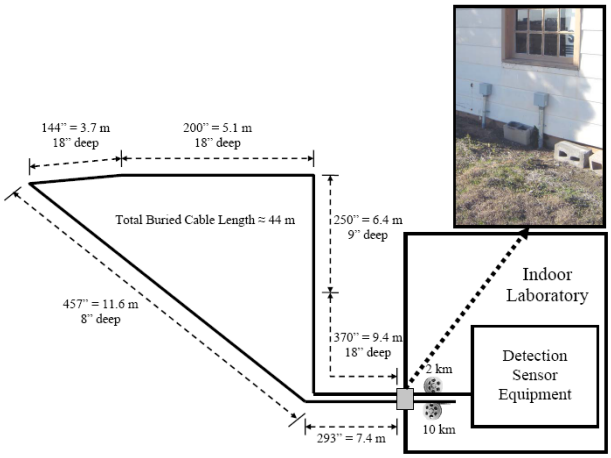

Fig. 4. Layout of fiber burial at Riverside. The conduits in the wall that the fiber passes through are also shown.

A paved road that carries automobile traffic runs next to the field, approximately 21 m from the fiber at its closest location. There is also a small dirt road that provides access to the indoor laboratory, which runs 4 m from the fiber at its closest location. These roads, which can be seen in Fig. 5, allow for testing vehicular intrusions.

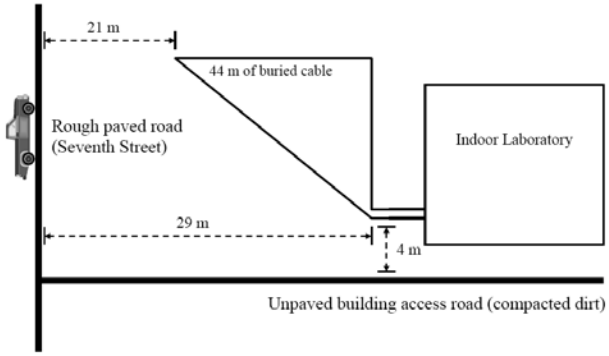

Fig. 5. Overall layout of test site at Riverside Campus.

CHAPTER III

INTRUSION DETECTION

LabVIEW software was used to program the FPGA to trigger the modulator to create the optical light pulses, continuously acquire data, process the data, and monitor the system for intrusions. Data is acquired at a rate of 1.5 MS/sec over two channels.

Intrusion location

Localization of intrusions along the length of the buried fiber is possible, and demonstrated in Fig. 6. Two consecutive periods of the backreflected signal are overlapped, with the difference between them shown. Knowing the time into this period that the difference occurs and the speed of light in the fiber, the location of the intrusion along the length of fiber can be determined.

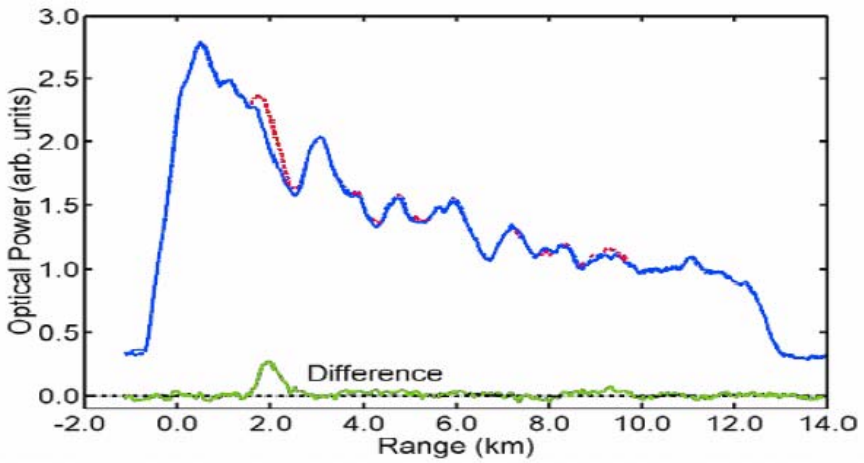

Fig. 6. Plot showing two consecutive pulses of the backreflected signal. Note that taking the difference between them allows for localization of intrusions.

Because of memory constraints on the FPGA, the entire length of optical fiber cannot be monitored for intrusions. In the test setup, only a short (44 m) section of fiber is buried, which can be treated as one point. As can be seen in Fig. 4, the buried fiber is located after a 2 km reel of fiber, so the area of interest is the 2 km point in the fiber. The pulse is introduced into the fiber at time t = 0, travels 2 km to reach this point in the fiber, and then the backreflected signal travels 2 km back to the detector. Therefore, the light must travel a total of 4 km, and the time required can be calculated by knowing the speed of light in the fiber, as shown in equation (1).

$$t = \frac{\ell}{v} = \frac{4km}{1.7x10^{8}\ {}^{m}\!/_{\text{sec}}} = 23.53\mu s \tag{1}$$

The sampling rate is 1.5 MS/sec. Knowing the time necessary for the optical signal from the 2 km point to reach the detector, the sample point to isolate out of each period can be determined, as shown in equation (2).

$$\text{Sample} = (\text{Sampling Rate}) \cdot (\text{Time Delay}) = \frac{1.5MS}{\text{sec}} \cdot 23.53\mu s = 35.29 \approx 35 \tag{2}$$

Therefore, to monitor the 2 km point in the fiber, the 35^{th} sample out of each period should be isolated. By isolating and comparing this data point over time, intrusions at the 2 km point can be detected.

This same premise can be used to monitor any location along the length of fiber. Equations (1) and (2) can be used to correlate a data point with any distance along the fiber. By isolating this data point, intrusions can be realized for that location.

Real-time signal processing

All signal processing is handled by the FPGA, which allows for real-time intrusion detection. A filter is used to remove noise, and then each data point is compared against a pre-programmed intrusion criterion as it is received. When the intrusion criterion is met, an intrusion signal is triggered.

The FPGA is programmed to constantly maintain a 10 second buffer of data. Once an intrusion signal is triggered, a timestamped data file is created, and the buffer immediately transferred into it. An additional 20 seconds of real-time data is added to the file. At the end of this time frame, the software resets itself, and waits for another trigger. The buffer and record times are both fully adjustable. In the case of an intrusion being triggered before the buffer has a full 10 seconds of data, the buffer is transferred to the data file, and enough real time data added to make a 30 second file.

Simulated intrusion

Before testing with actual intrusions, a piezoelectric cylinder (PZT) was used to confirm proper system calibration. The PZT has fiber wrapped around it and is located at the 2 km point, before the fiber exits through the conduit in the wall to be buried in the field.

By applying a controlled voltage to the PZT, the fiber is stretched and produces a phase shift. This allows for the creation of a simulated intrusion that can be duplicated.

With the program running, the PZT was used to create and record a simulated intrusion. The resulting signal can be seen in Fig. 7. Getting a signal confirms that the FPGA is triggering the laser pulse and acquiring data. In order to confirm that the correct data point out of each period is being isolated, the program was adjusted to isolate the data points on either side. In both cases, there was a 40% reduction in signal strength for the PZT intrusion, confirming data point isolation.

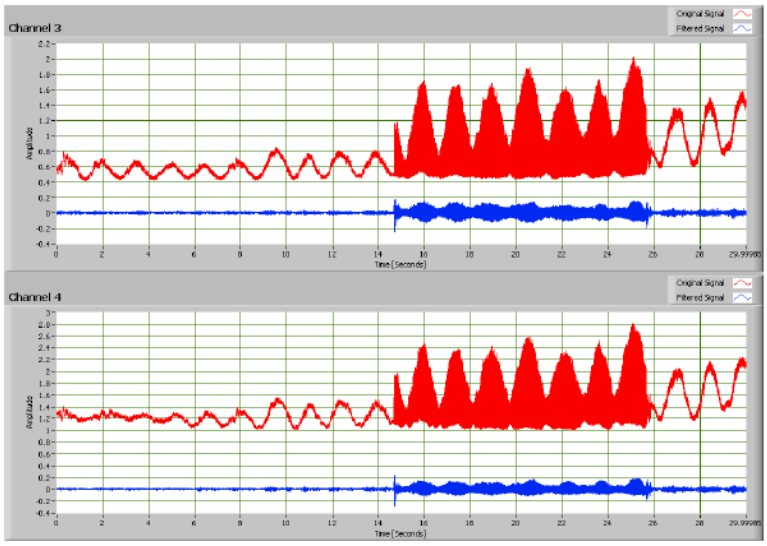

Fig. 7. Simulated intrusion created by the PZT at 2 km point along the fiber.

Triggered intrusion

After using the PZT to confirm proper program calibration, a real intrusion was made in the field. With the program running and waiting for an intrusion to trigger it, the test

field was walked. The triggered intrusion can be seen in Fig. 8. The first footstep is seen 10 seconds into the data file, which is due to the 10 second buffer that the program maintains.

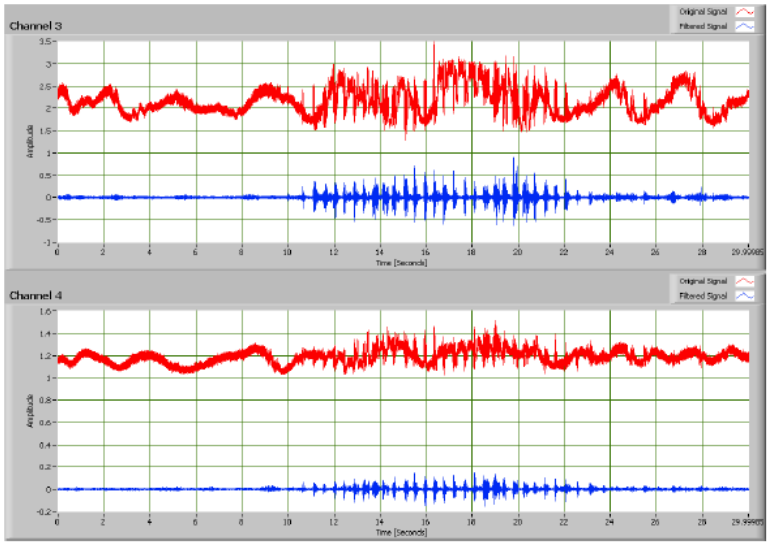

Fig. 8. Triggered intrusion file created by a human intruder on foot.

The software ends up creating a log of all the intrusions that have been triggered while it is running, and saves data files that can be viewed later for further analysis. A separate program is capable of plotting these files, giving the plots that are seen in the above figures. Note that both the raw and processed data is saved over two channels. Saving the raw data allows for more advanced signal processing algorithms to be run off-line if desired.

CHAPTER IV

INTRUSION SIGNATURE COMPARISON

In 2007, a paper was published on this intrusion system that gave detailed intrusion signature analysis for multiple intrusion types [10]. These results were obtained using off-line signal processing algorithms. While these are not real-time results, they do give a basis of comparison for the real-time results.

Single human intruder on foot

A single person walking across the buried cable can be seen in Fig. 9. The top plot (a) shows previous off-line results, while the bottom plot (b) shows results obtained with real-time FPGA signal processing.

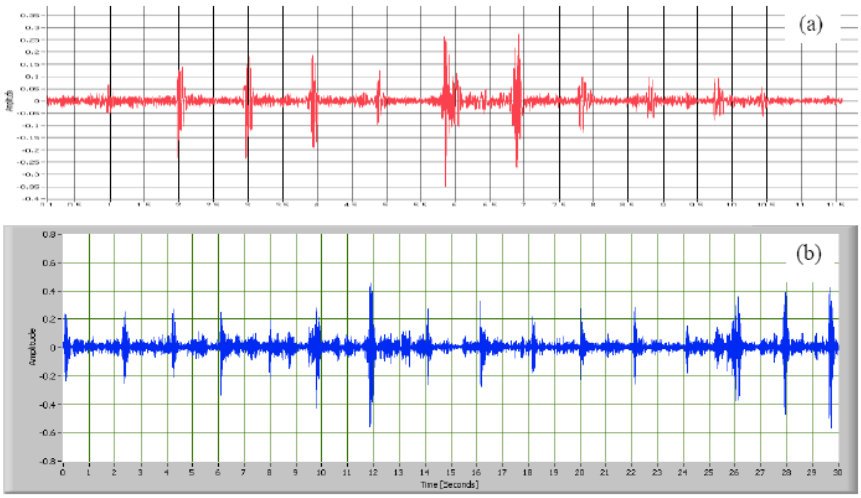

Fig. 9. Comparison of results from a human intrusion. Plots show a) Off-line data processing and b) Real-time FPGA data processing.

Individual footsteps are clearly identifiable in both cases. For the real-time intrusion, the field was walked at an angle, resulting in crossing directly over the buried fiber twice. This is confirmed in the plot, with the larger amplitude spikes resulting from being directly over the fiber. The FPGA real-time results are comparable to the off-line results, and real-time signal processing is desired.

It does appear that there is slightly more noise in the real-time processing case, which is probably due to the integer filter design. In the LabVIEW integer filter conversion, the integer filter did not exactly match the desired frequency response.

Vehicular intrusion

A 2004 Ford Ranger was used to make a vehicular intrusion, which can be seen in Fig. 10. The off-line intrusion signature was created with a four door compact car. The top plot (a) shows previous off-line results, while the bottom plot (b) shows results obtained with real-time FPGA signal processing.

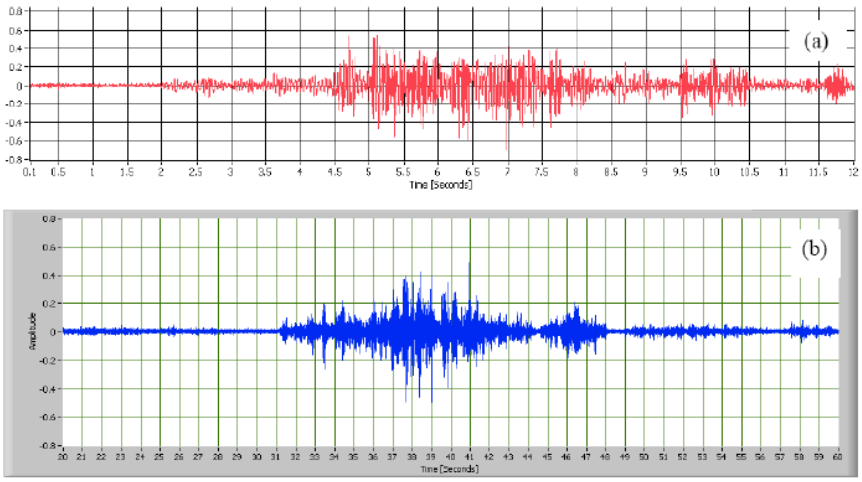

Fig. 10. Comparison of results from a vehicular intrusion. Plots show a) Off-line data processing and b) Real-time FPGA data processing.

A traveling car produces a continuous disturbance while the vehicle is within range of the buried optical fiber, with the amplitude of the disturbance being proportional to the distance from the fiber. Again, the FPGA real-time results are comparable to the off-line results, and real-time signal processing is desired.

CHAPTER V

SUMMARY AND CONCLUSIONS

A highly sensitive ϕ-OTDR system capable of detecting intruders near the vicinity of a buried fiber optic cable in real-time has been developed. Current research has focused on real-time signal processing algorithms to detect intruders and record their activity, utilizing a FPGA-based system. Field testing has shown successful results for monitoring one location along the length of fiber for intrusions. Real-time results were comparable to previous off-line signal processing results. The scalability of real-time signal processing over the entire length of fiber is limited by the amount of memory available on the FPGA unit.

Future work

Detection capability along the entire length of fiber is desired. The current program is capable of detecting intruders along the entire length of fiber, but can only monitor and record one location at a time. In the current program, this location is determined by a user defined input. Research is being done to scale up the software to give intrusion triggering and recording capabilities along the entire length of fiber.

Future research will also focus on developing next generation signal processing algorithms to improve the signal-to-noise ratio and to allow for instant classification of intruders. There is a lot of information to be mined from the raw data received by the

detectors. The current signal processing algorithm looks at the amplitude of the processed signal in triggering intrusions. It is believed that differences in frequency contribution can be isolated for intruder classification. This would be a desired feature for any security system.

This technology has demonstrated advanced sensing capabilities for low-cost perimeter monitoring. Numerous commercial and military applications exist for this technology in monitoring high-value and high-security targets. With the addition of several more key features, this technology will be ready for real world implementation.

REFERENCES

[1] National Institute of Building Sciences, "Provide security for building occupants and assets," <http://www.wbdg.org/design/provide_security.php>, 2007.

[2] Migration Policy Institute Staff, "Migration information source - The US-Mexico border," <http://www.migrationinformation.org/Feature/display.cfm?ID=407>, 2006.

[3] K. Shaneman and S. Gray, "Optical network security: Technical analysis of fiber tapping mechanisms and methods for detection and prevention," in *IEEE Military Communications Conference*, pp. 711-716, 2004.

[4] H. F. Taylor and C. E. Lee, "Apparatus and method for fiber optic intrusion sensing," Patent No. 5,194,847, 1993.

[5] J. C. Juarez, E. W. Maier, K. N. Choi, and H. F. Taylor, "Distributed fiber-optic intrusion sensor system," *Journal of Lightwave Technology,* vol. 23, pp. 2081-2087, 2005.

[6] K. N. Choi, J. C. Juarez, and H. F. Taylor, "Distributed fiber optic pressure/seismic sensor for low-cost monitoring of long perimeters," in *Proceedings of the SPIE, Unattended Ground Sensor Technologies and Applications V*, vol. 5090, pp. 134-141, 2003.

[7] J. C. Juarez and H. F. Taylor, "Distributed fiber optic intrusion sensor system for monitoring long perimeters," in *Proceedings of the SPIE, Sensors, and Command, Control, Communications, and Intelligence (C3I) Technologies for Homeland Security and Homeland Defense IV*, vol. 5778, pp. 692-703, 2005.

[8] J. C. Juarez and H. F. Taylor, "Polarization discrimination in a phase-sensitive optical time-domain reflectometer intrusion-sensor system," *Optics Letters,* vol. 30, pp. 3284-3286, 2005.

[9] National Instruments, "Introduction to FPGA technology: Top five benefits," <http://www.ni.com/fpga_technology >, 2006.

[10] C. K. Madsen, T. Bae, and T. Snider, "Intruder signature analysis from a phase-sensitive distributed fiber-optic perimeter sensor," in *Proceedings of the SPIE, Fiber Optic Sensors and Applications V*, vol. 6770, no. 67700K, 2007.

CONTACT INFORMATION

Name:	William Timothy Snider
Professional Address:	c/o Dr. Christi Madsen Department of Electrical and Computer Engineering MS 3128 Texas A&M University College Station, TX 77843-3128
Education:	B.S. Electrical Engineering, Texas A&M University, May 2008 Magna Cum Laude Undergraduate Research Scholar