Examining the Characteristics and Implications of Sensor Side Channels

Venkatachalam Subramanian*, Selcuk Uluagac*, Hasan Cam† and Raheem Beyah*

* GT-CAP, School of ECE
Georgia Institute of Technology
Atlanta, Georgia 30332, USA
venkat.subbu@gatech.edu, {selcuk, rbeyah}@ece.gatech.edu

†Network Science Division
U.S. Army Research Laboratory
Adelphi, MD 20783, USA
hasan.cam.civ@mail.mil

***Abstract*—The nodes in wireless sensor networks (WSNs) utilize the radio frequency (RF) channel to communicate. Given that the RF channel is the primary communication channel, many researchers have developed techniques for securing that channel. However, the RF channel is not the only interface into a sensor. The sensing components, which are primarily designed to sense characteristics about the outside world, can also be used (or misused) as a communication (side) channel. In this paper, we characterize the side channels for various sensory components (i.e., light sensor, acoustic sensor, and accelerometer). While previous work has focused on the use of these side channels to improve the security and performance of a WSN, we seek to determine if the side channels have enough capacity to potentially be used for malicious activity. Specifically, we evaluate the feasibility and practicality of the side channels using today's sensor technology and illustrate that these channels have enough capacity to enable the transfer of common, well-known malware. The ultimate goal of this work is to illustrate the need for intrusion detection systems (IDSs) that not only monitor the RF channel, but also monitor the values returned by the sensory components.**

Index Terms - Wireless Sensor Networks, Side Channels, Out-of-Band, Proximity Attacks

I. INTRODUCTION

The primary purpose of any Wireless Sensor Network (WSN) is to serve as a sensing-layer and an interface to the physical phenomena of the real world. The WSNs, which primarily consist of a number of autonomous sensors that collaboratively monitor physical and environmental conditions, have become ubiquitous, finding applications in the fields of military surveillance, environmental monitoring and health care systems. For instance, there are more than 400 sensors in a modern car that are used for monitoring various environmental parameters (e.g., temperature, light, pressure) [1]. Moreover, unmanned vehicles and armored suits used by the military also depend on a number of different environment-monitoring sensors (e.g., optical, acoustic, seismic, temperature). Similarly, sensor-based land mine detection systems are being continuously utilized in military scenarios with increased usage of the sensing components [2]. Given the importance and the increased usage of sensor-based applications, securing WSNs is vital.

There have been many solutions provided to secure WSNs. However, the overall security of WSN systems has focused only on the security of the radio frequency (RF) channel. Hence, many of the security frameworks for WSNs like [3], [4], and defense mechanisms against independent security attacks have been designed with respect to the RF communication channel.

In fact, sensory channels (e.g., light, acoustic, seismic) must also be considered in any security mechanism designed for WSNs. This is critical, because in addition to their use for benign applications, sensory channels can be utilized for malicious purposes. For instance, in smartphones, the visible light [5] and accelerometer [6] sensory channels have been used for benign purposes (authentication and key exchanges). On the other hand, a potential attacker could use the side channels to trigger or even transfer malicious code. For example, information can be encoded as a bit-stream consisting of ones and zeroes, which can be transmitted using an on-off pattern from a light source. When this light pattern is observed by the sensor, it is decoded to extract the information. Since most of the existing WSN security approaches only monitor the RF channel, sensors are still prone to *side channel* attacks corresponding to the specific sensing component in use.

In order to detect such side channel attacks and develop solutions to defend the WSNs against them, it is important to understand the characteristics of these side channels. In this paper, we provide an analysis of the feasibility and practicality of the side channels in terms of data rate and factors contributing to loss in these channels. Specifically, we evaluate these channels, for the first time, using real sensors. To the best of our knowledge, there is not an evaluation of WSN side channels. Our results show that, with today's sensor technology it is possible to use side channels for malicious purposes. Also, with further improvements in technology, the capabilities of these channels will be further accentuated. Accordingly, we discuss the need for and the general requirements for an IDS that monitors sensory channels. The contributions of our work are two-fold: we 1) analyze side channels to determine channel characteristics such as data rate and factors contributing to path loss using real sensors and 2) identify and exhibit malicious usage of the side channels.

The rest of the paper is organized as follows: Section II discusses the related work in terms of usage of side channels in WSNs. In Section III, an evaluation of individual side channels is presented. The malicious usage of side channels is exhibited in Section IV. Section V presents the performance evaluation of a possible malicious usage of the side channel.

978-1-4673-3122-7/13/$31.00 ©2013 IEEE

Then, Section VI discusses the need for a side channel specific IDS. Finally, Section VII presents the conclusions and future work.

II. Related Work

Various security solutions have been proposed to secure the RF channel of the sensors in WSNs. However, these existing techniques or solutions are vulnerable to *side channel* or *out-of-band* channel attacks. Although, to our knowledge, there have been little work that discusses vulnerabilities of and characterizes these sensory side channels, there have been several contributions that demonstrated the potential of these side channels to improve the security of WSNs [5], [7].

The Enlighten Me! [5] and KeyLED [7] approaches utilize the visible light channel (VLC) to improve the security in WSNs. However, both the approaches limit the usage of VLC to a secure key exchange protocol. Although, an attacker model is discussed in [5], it only focuses on the attacks against the key exchange procedure. In [8], secure initialization of WSNs using the VLC is illustrated. It proposes two protocols, one using secret key cryptography and the other using public key cryptography. Both protocols involve communication over a bidirectional radio channel and an unidirectional out-of-band VLC. However, similar to [5] and [7], [8] also limits the usage of VLC to authentication and key exchange procedures. On the other hand, approaches like [6] make use of the vibration channel for secure communication. This work exposes the weakness of a mobile application called *Bump* [9] that use the accelerometer values in mobile phones for authentication. Moreover, a secure authentication protocol using the vibration channel is described to overcome the drawback in *Bump*. Again, the vibration channel is used only for benign purposes.

The aforementioned contributions demonstrate the importance and potential usage of side channels in WSNs, analyzing different side channels. In this work, we provide an analysis of the performance of various side channels using real sensors, illustrate the malicious usage of the side channels and also highlight the need for a side channel based IDS. To the best of our knowledge, there is not an evaluation of WSN side channels.

III. Side Channel Analysis

In this section, we first introduce analytical models governing the path loss in side channels. Then, using real sensors we evaluate the feasibility and practicality of the side channels.

A. Side Channel Communication Models

Visible light, infrared, acoustic and seismic channels are identified as potential targets due to their ease-of accessibility.

1) Visible Light Channel: The visible light channel (VLC) is the most common side channel available in sensor systems. Almost all sensor platforms (e.g., Telosb, MicaZ, Iris) are equipped with a light emitting diode (LED) and most sensor boards (MTS310 [10], MTS400 [10], Telosb) have a photo-sensor. Also, military applications such as the *Airborne Laser Mine Detection Systems* [11] are based on light detection and ranging (LIDAR) which make use of the light channel. The data rate of such a VLC can be primarily characterized by two major factors, *sampling rate* of the sensor and *path loss* in the channel. The *sampling rate* or *bit rate* supported by the visible light sensors is entirely dependent on the specific sensor technology used.

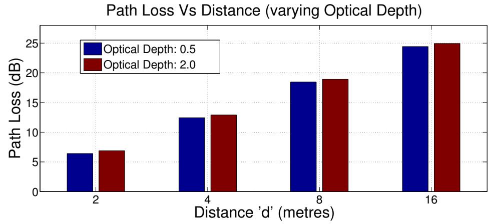

Fig. 1. Path Loss variations with respect to distance and optical depth

Besides the sampling rate, another parameter of significance which determines the quality of received light and impacts the capability of the VLC side channel is the *path loss*. The *path loss* in the light channel is calculated to quantify the overall effectiveness of the channel. According to the *inverse square law*, intensity, I_d, at a distance d is given by [12],

$$I_d \propto \frac{1}{d^2} \tag{1}$$

The path loss in decibels, L_l, can be given as [13],

$$L_l = A_t + L_a \tag{2}$$

where, A_t is the attenuation factor and L_a is the channel absorption loss. The attenuation factor in decibels, A_t, is determined by [13],

$$A_t = 20log\frac{d}{d_{ref}} \tag{3}$$

The second factor contributing to path loss is the channel absorption loss, L_a, which is given by [13],

$$L_a = e^{-\gamma} \tag{4}$$

where, γ is the optical depth of the channel. For an optically clear environmental condition, $\gamma \approx 0.5$ [13]. Therefore, the received light intensity (in decibels), R_i can be given as,

$$R_i = S_i - L_l \tag{5}$$

where, S_i is the light intensity of the source.

The variations of path loss, L_l, determined from the above formula, with increasing distance (d) and considering channels with different optical depth (γ) is shown in Figure 1.

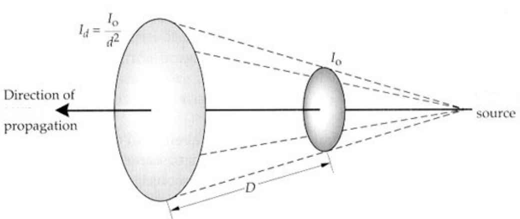

Fig. 2. Spherical Spreading Model for Acoustic Channel and VLC (from [14])

2) Acoustic Channel: The acoustic channel is another vital side channel and is widely used in various sensor systems. Similar to the VLC, data rate of the acoustic channel is also dependent on the supported *sampling rate* of the sensor and the *path loss* in the channel.

A spherical spreading model [14], as shown in Figure 2, is considered for determining the *path loss* in the acoustic channel, where, d is the distance between source and receiver, I_d is the intensity at the receiver and I_o is the intensity at the source. For estimating the resultant *path loss* (in decibels), the received sound level can be given as [15],

$$R_l = S_l - T_l \tag{6}$$

where, S_l is the sound level of the source and T_l is the transmission loss. The transmission loss (T_l) can be estimated by adding the effects of geometrical spreading (T_{lg}) and absorption (T_{la}), which is given as [15],

$$T_l = T_{lg} + T_{la} \tag{7}$$

According to the *inverse square law*, the sound intensity, I_d, at a distance d, is expressed as in Equation 1, Hence, the geometric spreading loss (T_{lg}) in Equation 7 is given by [15],

$$T_{lg} = 20log\frac{d}{d_{ref}} \tag{8}$$

Also, the absorption loss (T_{la}) in Equation 7 can be given by,

$$T_{la} = \alpha \times d \tag{9}$$

where, d is the distance in meters and α is the absorption coefficient which is a function of the frequency.

3) Seismic Channel: Accelerometers or seismic sensors are widely used in mobile phones and various robots. The seismic channel is potentially a more difficult channel and requires more sophisticated methods to exploit due to two main reasons. First, the level of proximity required to exploit this channel by an attacker is significantly higher compared to the visible light and acoustic channels. Second, a simple ON-OFF communication pattern would not be suitable for communicating with the accelerometers, which brings the need for a more sophisticated encoding/decoding technique. The data rate of the seismic channel also primarily depends on the *sampling rate* of the accelerometers and *attenuation* of vibrations (path loss) in the channel. A general expression for modeling propagation of ground vibrations can be given as follows [16]:

$$v_b = v_a(\frac{r_a}{r_b})^{\gamma} \; e^{\alpha(r_a - r_b)} \tag{10}$$

where, r_a, r_b are the distance of locations a and b, respectively from the source, v_a and v_b are velocity of vibrations at locations a and b, respectively, γ is a coefficient dependent on the type of propagation mechanism and α is the material damping coefficient. Similarly, the *attenuation factor*, A_t, is given by [16] as follows:

$$A_t = 20log(\frac{v_b}{v_a}) \tag{11}$$

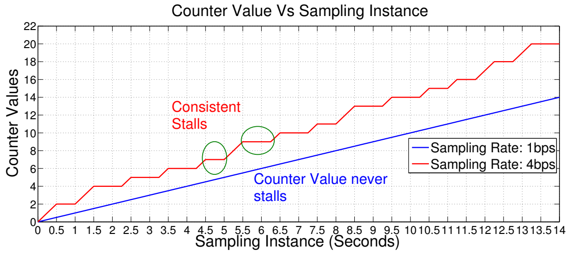

Fig. 3. Sampling Rate Experiment on VLC (using MTS420CC) - Counter Values

The attenuation factor, A_t, is used to estimate the attenuation of the vibrations at any point from the source. Therefore, the received intensity of vibrations, R_v, can be given as,

$$R_v = S_v - A_t \tag{12}$$

where, S_v is the intensity of vibrations produced by the source.

B. Side Channel Experiments

In this sub-section, we use real sensors to evaluate the feasibility and practicality of the side channels.

1) Visible Light Channel: Simple experiments conducted on Telosb and MicaZ (with MTS400CC [10] and MTS310CB [10]) motes illustrate the data rate of the VLC. An experiment was conducted to estimate the sampling rate of the different light sensors. We implemented a sensor application for the experiment that utilizes a simple integer counter. This application allows the sensor to sample ambient light at the specified sampling rate and checks for the value returned by the *event* in TinyOS. The value returned by the event denotes a *success* or *failure*. For every successful sampling, the counter is incremented. A stall in the counter value indicates that the sampling rate being used is beyond the capacity of the light sensor. Initially, the three different light sensors were allowed to sample continuously, every second (1 bps). Then, the sampling rate was gradually increased and the counter values were observed. It was observed that the MTS400CC sensor board experienced a stall in the counter values beyond a sampling rate of 3 bps as shown in Figure 3. Whereas, the MTS310CB sensor board and Telosb experienced a stall in the counter values beyond sampling rates of 65 bps and 100 bps, respectively. The observed sampling rates of the sensors (which influence the data rate of the channel) are tabulated in Table I. It is seen that Telosb motes which use the Hamamatsu S1087 visible light sensor support a much higher sampling rate (85-100 bps) than that of MicaZ with MTS400CC sensor board (2-3 bps) which uses the TAOS TSL2550D ambient light sensor. However, the MicaZ with MTS310CB sensor board (using CdSe photocell) is observed to have a reasonable *sampling rate* (50-65 bps).

2) Acoustic Channel: The data rate of the acoustic channel is also mainly characterized by the sampling rate of the sensor. We implemented an experiment similar to that of the VLC, with respect to the acoustic channel. The MTS310CB sensor board is used which utilizes a microphone to detect sound with frequency of 4KHz. A 4KHz buzzer is used to create continuous sound at 4KHz frequency. Again, the

TABLE I
SAMPLING RATE (OBSERVED) COMPARISON OF THE SIDE CHANNELS

Side Channel	Platform	Sensor Component	Observed Maximum Sampling Rate (bps)
VLC	Telosb	Hamamatsu S1087	85-100
	MicaZ (MTS400CC)	TAOS 2115	2-3
	MicaZ (MTS310CB)	CdSe Photocell	50-65
Acoustic	MicaZ (MTS310CB)	LM567 CMOS Tone Detector	2-3
Seismic	MicaZ (MTS310CB)	ADXL202JE Accelerometer	50-65

sensor application implemented increments a counter for every successful sampling. The counter value was observed to stall beyond a sampling rate of 3 bps. Thus, the sampling rate of the LM567 CMOS Tone Detector in MTS310CB was observed to be around 2-3 bps as shown in Table I.

3) Seismic Channel: We used the accelerometer in MTS310CB (ADXL202JE) for the sampling rate estimation experiment similar to the visible light and acoustic channels. The ADXL202JE is a dual-axis accelerometer and hence, both the X-axis and Y-axis were observed individually as well as together. The sensor was manually vibrated in a continuous manner. The sensor application similar to the one used in the VLC and the acoustic channel was modified such that it allowed the sensor to sample the accelerometers continuously and to increment a counter for each successful sampling. An occasional stall in the counter values was observed beyond 50 bps and a consistent stall in the counter values was observed beyond 65 bps. Thereby, indicating that the sampling rate of the accelerometer used is 50-65 bps (Table I).

4) Combination of Channels: With the experimental results from the individual channel analysis, one can determine a good combination of the different side channels. In this way, combining channels would enable one to produce a stronger attacker model. This would significantly increase the effective data rate and aid attacker scenarios like *Trojan Transfer* and *Secret Trigger* (discussed in the next section). Also, combined data from side channels can be intelligently handled using aggregation schemes like [17]. Moreover, in some conditions, some side channels may not be available for use. For instance, if the ambient visibility conditions are poor, then it would impact the performance of the light channel. In those cases, an algorithm may choose the best available side channel.

IV. MALICIOUS SIDE CHANNEL APPLICATIONS

This section presents malicious WSN applications or scenarios based on the side channels. Such WSN applications are primarily based on the fact that information can be transmitted over these side channels. For instance, information can be encoded as a bit-stream consisting of ones and zeroes, which can be transmitted using the on-off pattern from a light source. When this light pattern is observed by the sensor, it is decoded to extract the information. Apart from transmitting encoded information through these channels, they can also be utilized to simply signal a specific function or an embedded piece of malware. For instance, specific patterns of vibrations picked up by an accelerometer can be decoded and used as a trigger.

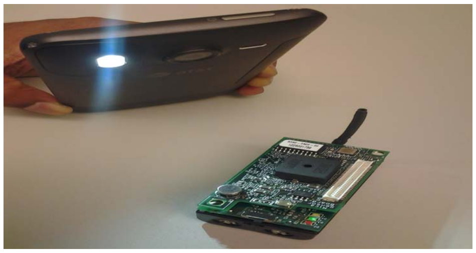

Fig. 4. Morse Code Experiment (Left: Android device; Right: MTS310CB with light sensors

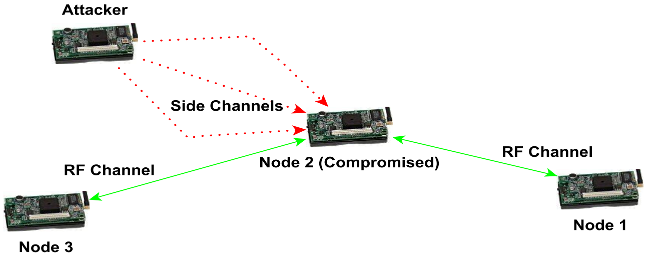

Fig. 5. Side Channel Attack in WSN with MicaZ sensors

A. Trojan Transfer

Sensors deployed in environments with moderate ambient light (e.g., cloudy day) and sound conditions (e.g., a conference room with 10 to 15 members) would support good data rates on these side channels and thereby become potential targets of side channel attacks. For instance, Figure 5 illustrates an attack scenario where an attacker uses the side channels to either transfer or trigger a trojan to/in the compromised node (node 2). This assumes that there exists a compromised node in the network as shown in Figure 5, which contains malware to decode information passed through side channels (e.g., visible light, acoustic, seismic). Then, a complete malicious code segment or trojan can be transmitted by the attacker through these channels. Since the primary RF channel remains unaffected by this attack procedure, it makes it more difficult to detect or prevent the attack. New trojans can also be transferred to the compromised node without being detected. This type of side channel attack is explained below using simple experiments.

1) Trojan Transfer using VLC: We implemented a sample *Morse code* encoder application (converts the input word to Morse code format) on the transmitter which was a HTC Inspire smartphone (Android-2.3.5) and a *Morse code* decoder application (converts Morse code to original format) on the receiver mote. This experiment mimics the *Secret Trigger* or *Trojan Transfer* scenario where an attacker would transmit similar encoded information over the VLC. This is performed in an environment with moderate ambient lighting. Figure 6 illustrates the decoded pattern using the MTS310CB for the

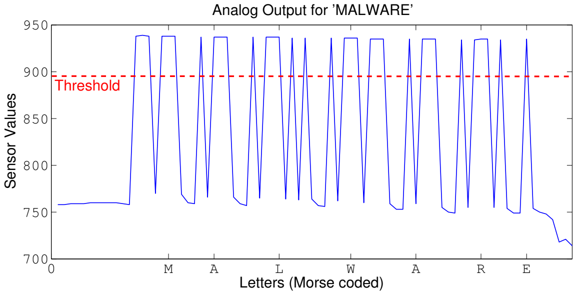

Fig. 6. Morse Code pattern for arbitrary data ('MALWARE') using VLC

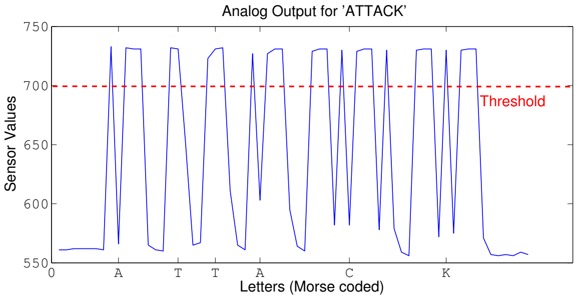

Fig. 7. Morse Code pattern for arbitrary data ('ATTACK') using Acoustic channel

transmitted random data 'MALWARE' (x-axis) using VLC readings (y-axis) from the sensor. Additionally, if infrared light channel is used instead of VLC, it provides a *concealed side channel* and thereby becomes more difficult to be detected.

2) *Trojan Transfer using Acoustic Channel:* For this experiment, a MicaZ mote with the MTS310CB sensor board is used. The microphone in the MTS310CB detects sounds with a frequency of 4KHz. The buzzer in the MTS310CB is used as the source which buzzes sound with a 4KHz frequency. Again, we implemented a *Morse code* encoder application (converting input to Morse code format) and a *Morse code* decoder application (converting Morse code to original format) on the buzzer mote and receiver mote, respectively. Figure 7 illustrates the decoded pattern using MTS310CB for the Morse encoded, arbitrary data 'ATTACK' (x-axis) using acoustic channel readings (y-axis) from the sensor. This can be extended by an equipped attacker to transfer a trojan over the acoustic channel. An advantage that the acoustic channel poses over the VLC is that the ambient noise can be neglected to a large extent by using a frequency which does not fall in the frequency range of the environmental noise.

For instance, in the experiment described above, a 4KHz buzzer is used and the detector is able to filter out only the 4KHz acoustic signals. Since the 4KHz frequency occupies only a small region in the audible frequency range (20Hz - 20KHz), the environmental noise in the audible frequency range did not have a large influence on our setup. Thus, similar the to VLC, the acoustic channel has the ability to provide a highly concealed side channel. When a frequency outside the audible frequency range is used, such as ultrasonic, it would become more difficult to be detected.

B. Secret Trigger

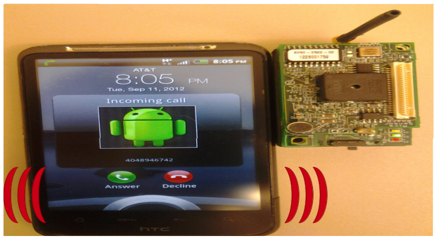

Fig. 8. Incoming Call Experiment (Left: Android device; Right: MTS310CB with accelerometers

It has been shown that devices may contain hardware trojans inserted by a determined vendor [18]. Hence, complimentary to the previous scenario, for sensors deployed in environmental conditions that limit the data rate of the side channels, the attacker can trigger a trojan or malicious code that was earlier stored in the target node. For instance, environments with high path loss would make it more difficult to perform attacks like Trojan Transfer. However, the attacker would still be able to use these side channels to trigger already stored trojans or trojans obtained over an RF channel without being detected. Furthermore, the compromised node's limited energy can be exhausted at a slower pace by activating the trojan when required and deactivating the trojan when not required using the side channels with reduced chances of being detected. Thus, the secret trigger mechanism can also be used as an *event-triggered* attack. For instance, by using the accelerometers in a compromised node, a trojan can be activated when the sensor becomes mobile due to a predetermined event. The trojan can be designed in such a way that the node starts transmitting sensitive information only when activated.

We designed and implemented a simple experiment to illustrate the *secret trigger* scenario. This experiment involved the accelerometers (ADXL202JE) in the MTS310CB sensor board which detects the vibrations produced by a mobile phone (HTC Inspire) running Android-2.3.5, during an emulated incoming call and use it as a trigger as shown in Figure 8. In order to mimic the incoming call vibrations, we also implemented a simple Android application for the Android-2.3.5 operating system. The duration of vibrations was chosen identical to that of an actual incoming call. Figure 9 shows the observed pattern in the accelerometer values during the experiment. The 'threshold region 1' shows the transition from a region with almost constant analog output (coded as bit stream of 0s) to the continuous increase in the accelerometer's readings (coded as a bit stream of 1s). This region indicates the start of the incoming call region. Similarly, 'threshold region 2' shows the transition from a continuously changing analog output to an almost constant value (a bit stream of 0s) or output with reduced variations. This region indicates the end of an incoming call' vibration pattern. This experiment shows that a potential attacker could use events such as an incoming call as a trigger by capturing the vibrations from the device.

C. Data Collection

The *Secret Trigger* scenario can be coupled with the default data collection functionality of the side channels and create a more advantageous scenario for an attacker. For example, the sensor network can be triggered by the attacker to collect sensor data during specific times.

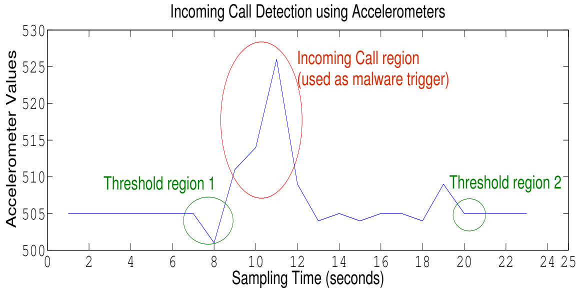

Fig. 9. Incoming Call Detection using an Accelerometer

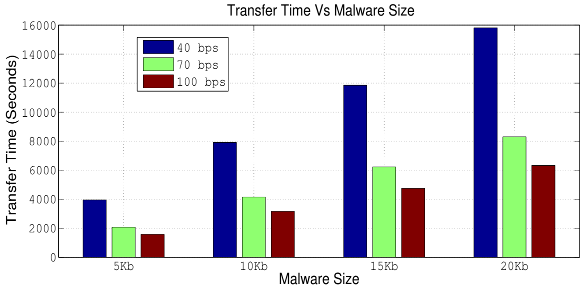

Fig. 10. Malware Transfer Time (using VLC)

V. Performance Evaluation

This section presents the performance evaluation of a malicious side channel scenario such as the *Trojan Transfer* along with measurements obtained from the experiment implemented for the evaluation.

As in the *Trojan Transfer* scenario described earlier, a potential attacker could possibly transfer an entire trojan through the side channels of the sensor node. In order to evaluate the effectiveness of such an attack over the VLC, we implemented a simple experiment to transmit *hex files* using a light source. The flashlight of a HTC Inspire (Android-2.3.5) smartphone was used for transmitting the Morse coded hex files. The hex files used in the experiment were chosen such that their sizes were comparable to those of existing malware samples [19]. Thus, we used four hex files, representing four different malware samples effectively (5Kb: Troj/JSRedir-BV, 10Kb: W32/Weird-L, 15Kb: Win32.jix, 20Kb: W32/Scribble-B) to measure the transfer time of each over VLC using *sampling rate* or *bit rate* of 40bps, 70bps and 100bps. A 5Kb hex file took approximately 3951.58 seconds to be transmitted at 40 bps, while the same hex file took approximately 2075.33 seconds to be transmitted at 70 bps and 1581.58 seconds at 100 bps. As expected, a relatively linear increase in the transfer time was observed with increase in the hex file size as shown in Figure 10.

VI. Side Channel IDS

From the side channel analysis and their malicious usage described in the earlier sections, it can be seen that the side channels are capable of carrying sufficient information or data for accomplishing such malicious activities or applications. Thus, the need for securing these channels is vital. However, the existing security solutions and IDSs are focused only on the RF channel. Therefore, the necessity for development of a side channel based IDS is evident.

Similar to IDSs for the RF channel, it would make sense to have a combination of signature- and anomaly-based techniques. The signature-based techniques would, for example, look for specific light patterns sensed by the photosensor to determine if a signature for malicious code was found. On the other hand, the anomaly-based technique would require each sensory components to develop a profile of normal sensed values and to monitor for deviations. For instance, the light pattern recorded by a photosensor while receiving a trojan is possibly different from the pattern recorded by the photosensor under normal conditions.

VII. Conclusion and Future Work

Myriads of solutions have been provided to secure WSNs, focusing only on the security of RF channel. In fact, sensory channels or side channels (e.g., light, acoustic, seismic) which are primarily designed to sense physical phenomena of the real world can also be used for malicious activities. Therefore, in this paper, we analyzed the side channels to determine the channel characteristics such as data rate and path loss using real sensors. We showed that sensory channels are capable of supporting malicious activities and also demonstrated their feasibility with various examples using today's sensor technology for the first time, to the best of our knowledge. Moreover, the need for side channel based IDSs is discussed along with early details on the design of such an IDS. In the future, we will investigate other side channels such as infrared, ultrasonic and magnetometer and develop a side channel based IDS.

Acknowledgment

This work was partly supported by NSF Grant No. CNS-1052769

References

[1] J. Stokes, "http://www.wired.com/autopia/2011/02/the-future-of-cars-p2p-mesh-4g-and-the-cloud/," *Wired*, 2011.

[2] A. Saurabh and A. Naik, "Wireless sensor network based adaptive landmine detection algorithm," in *Proc. of the 3rd IEEE ICECT*, April 2011.

[3] M. Valero, S. S. Jung, A. Uluagac, Y. Li, and R. Beyah, "Di-sec: A distributed security framework for heterogeneous wireless sensor networks," in *Proc. of the 31st IEEE INFOCOM*, March 2012.

[4] M. Valero, V. Subramanian, R. Kumbakonam Chandrasekar, Uluagac, and R. Beyah, "The monitoring core: A framework for sensor security application development," in *Proc. of the 9th IEEE MASS*, October 2012.

[5] M. Gauger, O. Saukh, and P. Marron, "Enlighten me! secure key assignment in wireless sensor networks," in *Proc. of the 6th IEEE MASS*, October 2009.

[6] A. Studer, T. Passaro, and L. Bauer, "Don't bump, shake on it: the exploitation of a popular accelerometer-based smart phone exchange and its secure replacement," in *Proc. of the 27th ACM ACSAC*, December 2011.

[7] R. Roman and J. Lopez, "Keyled - transmitting sensitive data over out-of-band channels in wireless sensor networks," in *Proc. of the 5th IEEE MASS*, October 2008.

[8] T. Perkovic, I. Stancic, L. Malisa, and M. Cagalj, "Multichannel protocols for user-friendly and scalable initialization of sensor networks," in *Proc. of the 5th ICST SecureComm*, September 2009.

[9] *Bump, http://bu.mp.*, BUMP Technologies.

[10] *MTS/MDA Datasheet, http://retis.sssup.it/sites/retis.sssup.it/files/Sensor*, Crossbow.

[11] C. J. Cassidy, "Airborne laser mine detection systems," Master's thesis, Naval Postgraduate School, Monetery, California, 1995.

[12] *Inverse Square Law, http://hyperphysics.phy-astr.gsu.edu/hbase/acoustics/invsqs.html*, Hyperphysics, GSU.

[13] L. C. Andrews, *Field Guide to Atmospheric Optics*. SPIE, 2004.

[14] *Spherical Spreading, http://www.life.umd.edu/faculty/wilkinson/bsci338/*.

[15] *Acoustic Monitoring, http://www.pmel.gov/vents/acoustic/tutorial/*, NOAA.

[16] G. CAUTES and S. NASTAC, "Mathematical model for frequency-dependent soil propagation analysis," in *The Annals of "Dunarea De Jos" University of Galati*, 2002.

[17] S. Ozdemir and H. Cam, "Integration of false data detection with data aggregation and confidential transmission in wireless sensor networks," *IEEE/ACM Transactions on Networking*, vol. 18, June 2010.

[18] L. Lin, M. Kasper, T. Güneysu, C. Paar, and W. Burleson, "Trojan side-channels: Lightweight hardware trojans through side-channel engineering," in *Proc. of the International Workshop on CHES*, September 2009.

[19] S. M. Tabish, M. Z. Shafiq, and M. Farooq, "Malware detection using statistical analysis of byte-level file content," in *Proc. of 15th ACM SIGKDD Workshop on CSI-KDD*, June 2009.