KeyLED - Transmitting sensitive data over out-of-band channels in wireless sensor networks

Rodrigo Roman, Javier Lopez
Computer Science Department
University of Malaga, Spain
roman,jlm@lcc.uma.es

Abstract

An "out-of-band" (OoB) channel can be defined as an extra channel, different from the main wireless channel, that has additional security properties. They are specially suitable for protecting spontaneous interactions and exchanging sensitive data between previously unknown devices. Due to the vulnerable nature of wireless sensor networks (WSN), these kind of channels might be useful for protecting certain sensor network operations. In this paper we analyze the applicability of "out-of-band" channels to wireless sensor networks, and specify why an optical channel should be a good candidate for implementing an extra channel in sensor nodes. Also, we analyze how the existing security threats may affect this type of channel. Finally, the suitability and usability of optical channels for sensor networks is demonstrated by means of a prototype.

Keywords - Wireless Sensor Networks, Out-of-Band Channel, Security.

1 Introduction

The main purpose of a Wireless Sensor Network (WSN) is to serve as the "sensing layer" of a computer system, an interface to the physical features of the real world. As a whole, the sensor network is able to continuously monitor its environment, adapting itself to the ever-changing context. There are many challenges to solve in the area of sensor networks, such as integration with other systems and services, architectural problems, programming models and tools, and others. But one of the most important challenges is security: any malicious adversary can manipulate the sensor nodes, the environment, or the communication channel on its own benefit. Precisely, "out-of-band" (OoB) channels are one of the technologies that could be used for protecting certain operations in a wireless sensor network.

Some of the existing research in personal area networks have already considered the importance of using "out-of-band" channels in sensor nodes. For example, Jea et. al. [1] use an optical channel (i.e. light as a transmission medium) for binding a device to the Body Sensor Network (BSN) of a certain user, and for transferring the ownership of the device from one BSN to another. Nevertheless, it is necessary to analyze whether "out-of-band" channels could be of use in a wireless sensor network context, and also if they could be implemented inside sensor nodes. These are the major goals of this paper.

The rest of this paper is organized as follows: In section 2 we introduce the specific features and different types of "out-of-band" channels. In section 3, we study the applicability of "out-of-band" channels to wireless sensor networks, alongside with a discussion of why sensor nodes should implement light "out-of-band" channels and what are the different security threats that may affect these optical channels (e.g long-distance attacks, denial of service (DoS), eavesdropping). In section 4 we develop a prototype, known as KeyLED, that demonstrates the suitability and usability of optical channels in sensor networks. Finally, in section 5, the conclusions are presented.

2   Existing "out-of-band" channels

"Out-of-band" channels have specific properties that distinguish them from the principal channels: their capabilities are usually limited (e.g. in most cases they are much slower than the principal channel), the devices (transmitter and receiver) need to be in a certain spatial relationship in order to establish communication, and the channels usually require the presence of a human user [2]. As a consequence from these properties, auxiliary channels can be useful for exchanging sensitive information. First, attackers may find extremely difficult to eavesdrop and / or modify the contents of the information exchange. Second, it is possible to assure in certain cases that the devices that exchange information through this auxiliary channel are physically near when communication takes place. Third, if a human user conducts the communication process, he/she can certify which is the sender device and which is the receiver device. There are many types of channels that can be used as "out-of-band" channels, such as *ultrasound*, *light*, *visual channels*, and even *human users*.

A human user can act as an "out-of-band" channel just by reading the output of one device and inputting this data in the other device. The hardware requirements of this type of channel are high: one device must have a display (LCD, sounder...), and another device must have an input mechanism. Also, the overall bandwidth provided by these channels is very constrained. On the other hand, both the sender and the receiver are directly controlled by the human user, and the usability of the schemes that employ this type of channel is high [3]. Moreover, there are other protocols that simplify the hardware requirements (e.g. by requiring only a single functional button in both sender and receiver [4], or by shaking the devices if they are equipped with accelerometers [5]). All these user-centric protocols are specially suitable for portable electronic devices, such as mobile phones. In this context, there are many well-known and effective protocols, like the Bluetooth Simple Pairing protocol.

The advantages of ultrasound as an "out-of-band" channel are discussed by Mayrhofer et. al. [6]. It can be safely assumed that ultrasound signals are unable to leave or enter a room, thus it is not possible to overhear or inject packets outside the room where nodes are deployed. Moreover, it can be possible to derive both the distance and the relative position of the sender using the time-of-flight and the angle-of-arrival, respectively. As a result, it can be possible to send authenticated short messages over these kind of channels inside a controlled environment (i.e. room), providing that the distance between the sender and the receiver is known.

McCune et. al. [7] take advantage of a visual channel, where the data to be transmitted is encoded as a two-dimensional barcode. The receiver takes a snapshot of the barcode with an embedded camera, and decodes it in order to obtain the secret information. Since the user needs to take a picture of the barcode attached or produced by the sender, it is assured that the barcode belongs to the sender, and that the receiver is obtaining the information from the right device. The visual communication paradigm may be not suitable for low-cost, embedded devices, due to the cost of the camera and the energy requirements of this type of channel. However, if light is used as a transmission medium, the receiver can utilize a simple photosensor (light sensor) instead of an expensive camera. This approach is taken by Jea et. al. [1] for binding a device to the Body Sensor Network (BSN) of a certain user, and for transferring the ownership of the device from one BSN to another.

3   Using OoB channels in WSN

3.1   Applicability

The inherent features of "out-of-band" channels could make them a particularly valuable technology for wireless sensor networks. If two nodes do not share any pairwise key, the security of the wireless communication channel is not assured. However, if the auxiliary channel is particularly difficult to manipulate or eavesdrop, two previously unrelated nodes can be able to share sensitive information with each other. Moreover, if a node receives information through these auxiliary channels, it can safely assume in most cases that the communication source is physically near. In order to confirm how these properties can benefit a sensor network, it is necessary to analyze whether "out-of-band" channels are actually useful for securing specific sensor network operations.

Pre-deployment phase. It could seem that there is no need for auxiliary channels when the sensor nodes are being programmed before their deployment. Any relevant information, including security credentials, can be preloaded in a safe environment through wired interfaces (e.g. using USB connections). However, for usability reasons, it can be possible to use an "out-of-band" channel to load the motes with application-specific information or with node-specific sensitive information. For example, a programming device can be used for generating the private key of a

node and its associated public key, alongside with the certificate signed by the Certification Authority (CA). Later, this device can transmit this information through the "out-of-band" channel to the sensor node. This is useful for providing configuration parameters "on-site" to nodes that are being deployed in potentially unsafe environments (i.e. there could be an adversary listening to the wireless channel).

Network extensibility. An "out-of-band" channel is specially useful whenever new nodes are added to an existing sensor network. The new node and the existing node can set up a security association through a pairing process [3], establishing a pairwise key. If the auxiliary channel and the environment are secure enough, the new node can directly send an ephemeral secret key to the existing node, which will use the key for any subsequent negotiations. This is applicable to certain configurations of the ZigBee standard, where the keys are set up over-the-air. Furthermore, it can be possible for the new node to send non-sensitive information such as public key certificates. While this kind of information can be safely sent through the wireless channel, by using the auxiliary channel it is possible to assure that the new node is physically near the existing node. Note that the use of an "out-of-band" channel does not assure that the new node really belongs to the network, thus it is still necessary to include authentication mechanisms.

Network maintenance. There exist some network maintenance operations that can take advantage of the features provided by "out-of-band" channels. For example, a mobile base station can use the auxiliary channel to issue orders to a certain node, or the node may send certain values of its configuration back to the mobile base station. As messages are not broadcasted through the wireless channel, it is not possible for an outsider device to detect their existence. As a result, an auxiliary channel can be used to protect the location privacy (i.e. detect the whereabouts of a node based on its network activity) and content privacy (i.e. infer the contents of a message based on its existence) [8] of a node. As with the network extensibility, there is the need of using authentication mechanisms in unsafe environments.

3.2 Light "out-of-band" channel

As aforementioned, "out-of-band" channels can be used in a wireless sensor network context for preloading information, adding new nodes in the environment, and performing some network maintenance operations. However, in order to take advantage of these type of channels, it is necessary to decide which of the existing components of a sensor node could be used to create an auxiliary channel. Almost all sensor platforms are equipped with a simple communication device: a light-emitting diode (LED). Moreover, most sensor nodes are also equipped with a photosensor. Therefore, a wireless sensor network can use these components to create an unidirectional "out-of-band" channel.

The light of a LED can be used as a carrier wave, and the digital data can be represented as the presence or absence of the carrier wave ("On-Off Keying", OOK). The photosensor will conduct a current that depends on the detected light intensity, and this current will be further converted to Lux (unit of illuminance). The maximum data rate of this light "out-of-band" channel is highly dependant of the speed of the LEDs and the photosensors used in the sensor node. LEDs are very fast; that is, they exhibit a quick response (tens of nanoseconds) to changes in the applied drive voltage. On the other hand, photosensors need more time to detect the light intensity of the environment. The maximum speed will be limited, then, by the speed of the photosensor.

Regarding the transmission range, the LEDs used in sensor nodes are not prepared to use their light as part of a communication channel due their large divergence angle (i.e. the light beam is not narrow), which results on a large loss of power between the sender and the receiver. Besides, the transmission channel is especially prone to be affected by various noise sources, such as ambient light. For example, the approximate luminous flux of a sensor node LED is 0.05 lumens[1], whereas a standard 60W bulb light has a luminous flux of 710 lumens [9]. As a consequence, the transmission range of a light "out-of-band" channel is limited to several centimeters. Nevertheless, this is not a drawback but an advantage: it assures that the sender and the receiver will be physically near when communication takes place, which is one of the fundamental characteristics of "out-of-band" channels.

Another factor that must be taken into account is the activation of the communication channel. Due to energy constraints, it is not feasible to continuously use the photosensor to sense any information that could be encoded in the incoming light intensity. Besides, the sender must be notified that there is data to be sent through its LEDs. It is then necessary to use the hardware available to the sensor node to indicate both senders and receivers that they should start sending and receiving data, respectively. Consequently, a human user needs to be physically interacting with the hardware of the motes, which satisfies one of the properties of "out-of-band" channels (human involvement in the communication process).

If the sensor nodes are equipped with user buttons (e.g. TelosB motes), it is possible to activate the channel simply by pushing such buttons. On the other hand, if the sensor node has no buttons, it is still possible to use some of the

---

[1]Note that one lux is equal to one lumen per square metre.

sensors to activate the channel. For example, certain motes (e.g. MICAz sensor boards) have accelerometers, thus it is possible to 'shake' the nodes to begin the communication process. Note that it can be also possible to activate the communication channel on the receiver side by requiring the sender to send a message through the principal channel (e.g. through a radio frequency transceiver). A problem of this approach is how to assure that the sender is physically near from the receiver. However, by using certain parameters such as Link Quality Indicators (LQI), the receiver can check if the distance between both devices is smaller that 2 or 3 meters (cf. figures in [10]).

3.3   Security Analysis

The security of light as a transmission medium is as weak as any other wireless channel: light is easy to capture and easy to produce. Therefore, it is necessary to analyze how the existing security threats may affect this type of channel in a sensor network context.

Regarding message injection attacks, as pointed out in section 3.2, in most cases a human user must activate the communication channel by touching the sensor nodes (pressing buttons, shaking devices). Therefore, these injection attacks could only be performed when a legitimate user is trying to start a communication channel between two devices. With the actual state of the art in optical wireless communications, it is possible to create long-distance communication channels through an atmospheric channel using visible-light diodes or laser diodes [11]. Nevertheless, in most of these scenarios, it is necessary to have a lens in he receiver side in order to condense the photonic area down to the size of the detector area. Moreover, there must be an unobstructed view between the light emitting device of the attacker and the photosensor of the node. In order to further reduce the possibility of attacks, the light "out-of-band channel" can use a photosensor that is not sensitive to infrared radiation.

Another possible attack that may affect light "out-of-band" channels is the denial of service attack (DoS). In order to disrupt the communications between two nodes, the attacker must influence over the light intensity perceived by the photosensor. Ambient light is the most important source of interference and it may greatly deteriorate link performance. Consequently, the attacker can try to alter the existing ambient light with the purpose of increasing the bit error of the channel. Moreover, the attacker can try to "blind" the photosensor during the communication process by using any of the communication methods introduced in the previous paragraph (i.e. laser light). However, since a human user needs to control the sender and the receiver in order to establish the communication channel, he/she will be able to detect any light beams or changes in the ambient light that try to interfere with the communications. And if the attack succeeds, the human operator can try to start the communication again.

Lastly, the attacker can try to sense the light emitted by the LED in order to eavesdrop the contents of the message. Due to factors such as the critical flicker frequency of the human eye [12], attackers should use recording devices (e.g. videocameras) to capture the information. As of 2008, some professional digital video cameras can achieve a frame rate of 1000 fps, which is good enough to capture the variations in the light intensity of the LED. On the other hand, just by using converging lens and optical bandpass filters it can be possible to sense and decode the contents of a light communication channel. Experiments performed by Loughry and Umphress [13] showed that the logical information contained within the light can be read from a distance of 30 meters.

The risk of eavesdropping can be lowered by using simple countermeasures. A human operator controls the nodes during the communication process, thus he/she can limit the optical emanations during the information exchange either by choosing a suitable environment (e.g. a closed room) or by covering the nodes (e.g. using a box, his/her hands). Regarding optical bandpass filters, since they cannot sense frequencies outside their working range, it can be possible to use more than one LED to transmit the information. For example, a typical sensor node has three LEDs: red, green, and blue/yellow. If those three LEDs are used alternatively to transmit the information (*ith bit* red, *i+1th bit* green, *i+2th bit* yellow/blue), a device equipped with a single optical pass filter will not be able to capture all the information.

4   Implementing "out-of-band" light channels in sensor nodes

4.1   Implementation and Experiment

The feasibility of an "out-of-band" light channel in a sensor network environment is tightly related to its transmission speed and its memory consumption. Since a human operator needs to directly control the sender and the receiver nodes, any unnecessary delays will make the whole process tiresome and unviable. Also, the memory available to a node is very limited, so the component that implements the transmission and reception algorithms should use only
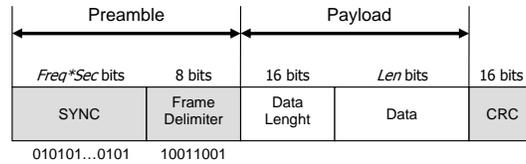
Figure 1. Format of the KeyLED data frame

a small amount of memory. In order to test the applicability and usability of light-based "out-of-band" channels in sensor networks we have developed a proof-of-concept prototype called *KeyLED*, using TinyOS 2.0 and the TelosB family of sensor nodes. This prototype works as follows:

1. The receiver node starts reading its light sensor (a Hamamatsu S1087) after the human user pushes the user button.

2. The sender node starts sending information through its blue LED after the human user pushes the user button. The information data is modulated by using an On-Off Keying (OOK) modulation scheme, where the presence or absence of light will be considered as "1" or "0", respectively.

3. The human user puts the LEDs of the transmitter in front of the light sensor of the receiver. The information data is sent from one node to another through the atmospheric channel. Note that the light communication channel use a fixed data rate that is known in advance to both sender and receiver.

The format of a KeyLED data frame is shown in Fig. 1. As the human user needs to bring near the LEDs and the light sensor, it is necessary to use a *SYNC* block that will alert the light sensor of an incoming data frame. The SYNC block, of variable length, is formed by continuously repeating the "01" pattern. The length of this field can be adjusted for giving time to the user to put the LEDs in front of the light sensor. The end of the SYNC block is signalled by a 8-bit *Frame Delimiter*, with value "10011001". This value breaks the pattern of the SYNC block, effectively indicating the beginning of the packet payload. This payload consists of a 16-bit *data length* field, and a variable length *data* field. Finally, at the end of the data frame, there is a 16-bit *CRC* field which detects accidental alteration of data during transmission. We use the CRC-16-CCITT standard in the prototype.

The usability and reliability of the KeyLED prototype was determined by two experiments. In the first experiment, 12 test subjects with no previous experience with the prototype were asked to send information from mote to another using the light "out-of-band" channel under fluorescent illumination. In the second experiment, we tested the channel under varied illuminance conditions. In both experiments, a ECC Public Key was sent through the "out-of-band" light channel with a raw bitrate of 500bps and a SYNC size of 1500 bits (i.e. three seconds). The size of the public key was 352 bits, as in Wang et. al. ECC implementation [14].

For the first experiment, the success ratio was 100%. The arithmetic mean of the number of attempts per person was 2.166, with a standard deviation of 0.799. Regarding the second experiment, the light channel does not work if the sensor node is deployed under direct sunlight (3400 lx), due to the low luminance of the LED. However, the channel is able to transmit the public key under all the other ambient light conditions, from clear night (4 lx, transmission range of 6 cm) to cloudy day (2700 lx, direct contact). As a result, it is possible to use this light channel on sensor nodes in most scenarios. Besides, the user can lower the ambient noise, that is, the high illuminance produced by the light of the sun, by covering the sensor nodes.

4.2 Discussions

In terms of memory consumption and speed, a light "out-of-band" channel is feasible and usable in a sensor network context. The memory consumption of the KeyLED prototype if not high: the KeyLED transmitter component consumes 54B of RAM and ~1kB of ROM, while the KeyLED receiver component consumes 126B of RAM and ~5kB of ROM. In addition, the theoretical maximum raw bitrate of this communication channel in a TelosB node is ~1300bps, and in an experimental setting the channel is able to achieve speeds as high as 500bps. Still, there are some aspects of the prototype that need to be discussed: why the blue LED has been used for sending the information, and how the receiver can convert the illuminance values into digital 0s and 1s.

In the KeyLED prototype, we use the blue LED for transmitting the information. Using the blue LED is not an arbitrary decision: This LED provides a luminous intensity of 14 millicandela (mcd), whereas the red LED and the green LED provide only 11.7 mcd and 6.4 mcd, respectively. The luminous intensity is not the only factor that must be taken into account: the S1087 photodiode reaches its maximum sensitivity at around 555 nm (540 THz), in the green region of the optical spectrum. Still, the green LED does not have enough luminous intensity to induce a high current in the photodiode. This assumption is backed up by empirical results. Upon direct contact between the LED and the photosensor, The blue LED produces an illuminance of 3000 lx, while the green LED and the red LED produce an illuminance of 1700 lx and 2500 lx, respectively.

As the light channel uses On-Off Keying, it is essential to establish which light intensity values must be considered as 0 and as 1. However, the ambient light is not constant during the lifetime of the network, and in some cases (e.g. fluorescent lights) the illuminance may fluctuate when two nodes open a communication channel. Therefore, it is necessary to analyze the light intensity of the environment before the real communication takes place in order to select a suitable threshold.

The receiver can perform this task during the reception of the SYNC block. The receiver will consider the illuminance sensed by the photosensor as 0 if it is smaller than the previous reading, and viceversa. During this process, it is possible to store the maximum illuminance values for the 0's ($maxmin$), and the minimum illuminance values for the 1's ($minmax$). After receiving the frame delimiter "10011001", the node can calculate the following threshold:

$$threshold = maxmin + \frac{minmax - maxmin}{2} \tag{1}$$

During the communication process, when the photosensor receives an illuminance value that is higher that the threshold it will translate such value as a digital 1, and viceversa.

5 Conclusions

In this paper, we have discussed the role of "out-of-band" channels in wireless sensor networks for exchanging sensitive information. We have considered that most sensor nodes are capable of using their LEDs and photosensors to create an optical channel, and we have studied both the possible applications of this channel and the security implications of using light as a transmission medium. Finally, we have presented a prototype, KeyLED, for testing the suitability and usability of light "out-of-band" channels.

One of the benefits of using a light "out-of-band" channel in sensor networks is the possibility of receiving information from virtually any light-emitting device (e.g PDAs). This interaction between heterogeneous devices can be very important for securing a pervasive computing environment like body sensor networks. Still, there are some challenges (e.g. dynamic negotiation of the bitrate) that will have to be solved in future developments.

Acknowledgements

References

[1] D. Jea, I. S. Yap, M. B. Srivastava. *Context-aware Access to Public Shared Devices*. In proceedings of the 1st International Workshop on Systems and Networking Support for Health Care and Assisted Living Environments (HealthNet 2007). San Juan (Puerto Rico), June 2007.

[2] D. Balfanz, D. K. Smetters, P. Stewart, H. C. Wong. *Talking to strangers: Authentication in ad-hoc wireless networks*. Proceedings of the 2002 Network and Distributed Systems Security Symposium (NDSS02), San Diego (USA), February 2002.

[3] E. Uzun, K. Karvonen, N. Asokan *Usability Analysis of Secure Pairing Methods*. Proceedings of the 1st International Workshop on Usable Security (USEC 2007), Scarborough (Trinidad and Tobago), February 2007.

[4] C. Soriente, G. Tsudik, E. Uzun. *BEDA: Button-Enabled Device Pairing*. Proceedings of the First International Workshop on Security for Spontaneous Interaction(IWSSI 2007), Innsbruck (Austria), September 2007.

[5] R. Mayrhofer, H. Gellersen. *Shake Well Before Use: Authentication Based on Accelerometer Data*. Proceedings of the 5th International Conference on Pervasive Computing (PERVASIVE 2007), Toronto (Canada), May 2007.

[6] R. Mayrhofer, H. Gellersen. *On the Security of Ultrasound as Out-of-band Channel*. Proceedings of the 21st IEEE International Parallel and Distributed Processing Symposium (IPDPS 2007), Long Beach (USA), March 2007.

[7] J.M. McCune, A. Perrig, M.K. Reiter. *Seeing-is-believing: using camera phones for human-verifiable authentication*. Proceedings of the 2005 IEEE Symposium on Security and Privacy, Oakland (USA), May 2005.

[8] C. Ozturk, Y. Zhang, W. Trappe, M. Ott. *Source-location privacy for networks of energy-constrained sensors*. Proceedings of 2nd IEEE Workshop on Software Technologies for Future Embedded and Ubiquitous Systems (WSTFEUS'04), Vienna (Austria), May 2004.

[9] OSRAM GmbH. *OSRAM CLASSIC Standard A Light Bulb, 60W 230V E27 FS1*. http://www.osram.com

[10] J. Blumenthal, R. Grossmann, F. Golatowski, D. Timmermann. *Weighted Centroid Localization in Zigbee-based Sensor Networks*. Proceedings of the 2007 IEEE International Symposium on Intelligent Signal Processing (WISP 2007), Alcala de Henares (Spain), October 2007.

[11] Twibright Labs. *Ronja (Reasonable Optical Near Joint Access)*. http://ronja.twibright.com/

[12] T.J. Andrews, L.E. White, D. Binder, D. Purves. *Temporal Events in Cyclopean Vision*. Proceedings of the National Academy of Sciences of the United States of America, vol. 93, no. 8, pp. 3689-3692, April 1996.

[13] J. Loughry, D.A. Umphress. *Information Leakage from Optical Emanations*. ACM Transactions on Information and System Security, vol. 5, no. 3, pp. 262289, August 2002.

[14] H. Wang, B. Sheng, C. C. Tan, Q. Li. *WM-ECC: an Elliptic Curve Cryptography Suite on Sensor Motes*. Technical Report WMCS-2007-11, College of William & Mary, October 2007.