Chapter 5

# SECURING DATA IN POWER-LIMITED SENSOR NETWORKS USING TWO-CHANNEL COMMUNICATIONS

Clark Wolfe, Scott Graham, Robert Mills, Scott Nykl and Paul Simon

**Abstract** Confidentiality and integrity of wireless data transmissions are vital for sensor networks used in critical infrastructure assets. While the challenges could be addressed using standard encryption techniques, the sensors are often power-limited, bandwidth-constrained or too rudimentary to accommodate the power and latency overhead of robust encryption and decryption implementations. To address this gap, this chapter proposes a novel methodology in which data is split between two distinct wireless channels to achieve acceptable levels of data confidentiality and/or integrity. Threat scenarios are discussed in which an attacker gains access to one of the two communications channels to either eavesdrop on or modify data in transit. Given these threats, five data splitting methods are presented that employ the two-channel communications concept to detect and adapt to the attacks, and provide varying levels of data security. Additionally, a simple proof-of-concept packet structure is introduced that facilitates data transmission over the two channels in accordance with the data-splitting methods.

**Keywords:** Wireless sensor networks, data security, two-channel communications

## 1. Introduction

Data security includes the challenge of protecting data in transit from eavesdropping and unauthorized tampering such as data modification. Normally, this challenge is met by applying encryption in the form of industry-standard symmetric-key algorithms such as the advanced encryption standard (AES). However, for small, low-powered devices, such as those used in remote sensor networks, the additional computational resources required for robust encryption may consume more power and time than are acceptable [4]. This chapter presents a proof-of-concept methodology that partially mitigates eavesdrop-


J. Staggs and S. Shenoi (Eds.): Critical Infrastructure Protection XII, IFIP AICT 542, pp. 81–90, 2018.
https://doi.org/10.1007/978-3-030-04537-1_5

ping and data modification threats using two-channel communications while reducing the encryption overhead.

## 2. Background

This section briefly discusses the threats to data in transit, the overhead imposed by encryption and the concept of two-channel communications.

### 2.1 Data Threats

A sensor network is an interconnected system of small sensors, each containing computing and communications elements. Sensor networks are used in numerous industries to monitor conditions or control equipment in remote locations. They often comprise large numbers of low-powered devices that are designed to conserve battery life while communicating critical information over wireless links [2].

Because of their wireless nature, sensor networks face a multitude of attacks. This work focuses on two types of man-in-the-middle (MiTM) attacks: (i) eavesdropping; and (ii) data modification. Eavesdropping is the unauthorized interception of confidential data. In the case of a wireless sensor network, eavesdropping could occur by placing an unauthorized receiver within signal range of the sensor network to collect transmitted data [6]. In a data modification attack, a network intruder modifies the data after it is sent, but before it reaches the intended recipient [5].

### 2.2 Encryption Overhead

Encryption provides confidentiality at the cost of computational resources such as memory, power and time. Wireless sensor networks typically have limited computational and power resources and, therefore, modern encryption standards such as 128-bit AES can impose significant burden on individual nodes. According to one study [7], using 128-bit AES to encrypt just one 128-bit block of data required 946 bytes of random access memory (RAM), 23.57 $\mu$J and 1.1 ms on an IEEE/ZigBee 802.15.4 board commonly used in low-power wireless sensor networks. These resources add up quickly as increasing amounts of data are transmitted over the lifespan of the sensor. For example, according to the following equation:

$$1GB \times \frac{8\,\text{bits}}{1\,\text{byte}} \times \frac{23.57\,\mu\text{J}}{128\,\text{bits}} \times \frac{1\text{Wh}}{3600J} = 0.41\text{Wh} \quad (1)$$

a sensor encrypting one GB of data would expend 0.41 Wh of energy just to encrypt the transmitted data. Such power consumption would significantly affect battery life in a device that may have a few watt-hours of energy.

Lightweight encryption schemes, such as the SIMON and SPECK encryption ciphers, attempt to address this issue in low-powered devices by offering more efficient, but less robust encryption options [1]. However, no encryption


*Figure 1.* Policy development process.

scheme can eliminate the overhead completely. Fortunately, the two-channel communications concept presented in this chapter can achieve adequate levels of data confidentiality and integrity without introducing significant encryption overhead.

## 2.3 Two-Channel Communications

As its name suggests, the two-channel communications technique transmits data over two channels in order to increase the security profile of data in transit. A simple example is a wireless network operating over the 2.4 GHz and 5 GHz industrial, scientific and medical (ISM) radio bands. The proposed methodology for a wireless sensor network requires each sensor to be equipped with full-duplex communications over two data links with distinct frequencies. The two-channel data splitting occurs at the physical layer, which enables industry-standard data transmission protocols to ride on top of the two-channel implementation.

The methods utilized to split data between the two channels operate under the assumption that the attacker has gained access to only one of the two channels. This is because the situation where an attacker successfully targets both communications paths reduces to the single-channel man-in-the-middle attack scenario. For simplicity of analysis, it is assumed that the two channels have the same bandwidth. Finally, while the methodology could be applied to any number of channels, the focus is on two channels for reasons of simplicity.

# 3. Proposed Methodology

This section describes the proposed two-channel methodology in which data is split between two distinct wireless channels to achieve acceptable levels of data confidentiality and/or integrity.

## 3.1 Threat Scenario Development

The first step in developing the two-channel solution for combating eavesdropping and data modification attacks is to model the threat scenarios. Following this, the techniques for mitigating the attacks are developed. Finally, the mitigation techniques are specified in terms of two-channel policies that leverage both channels to reduce or eliminate the threats. Figure 1 summarizes the policy development process.

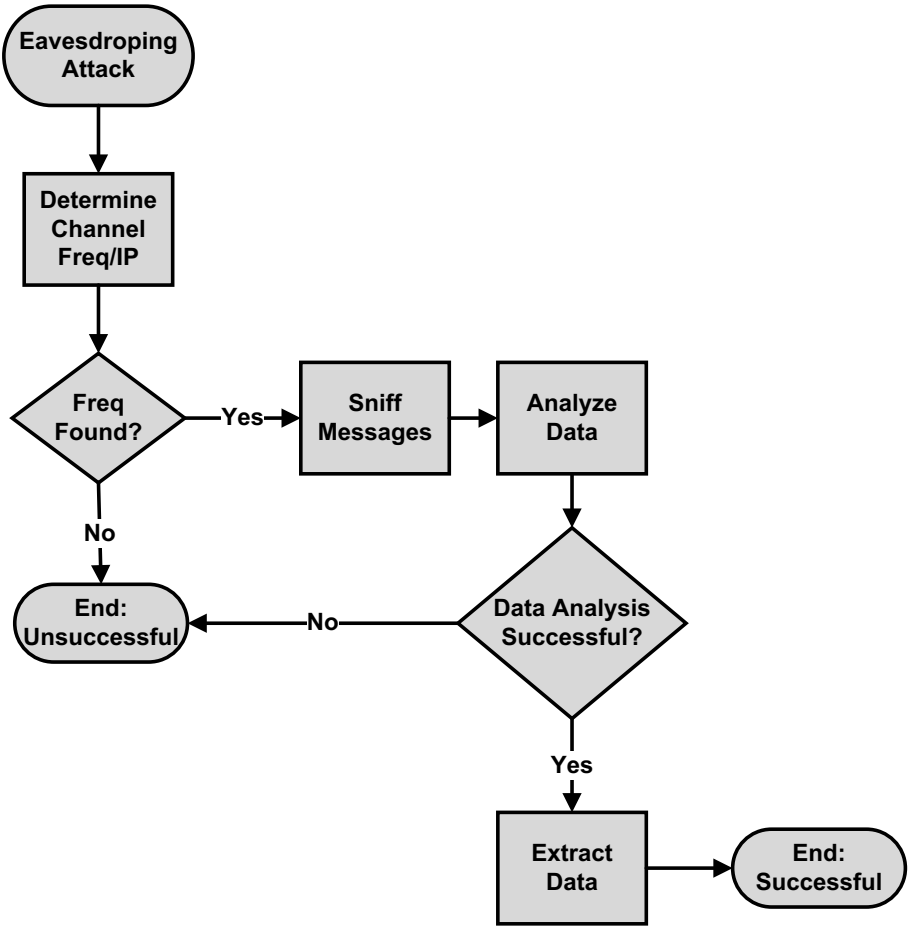


*Figure 2.* Eavesdropping attack.

## 3.2 Eavesdropping Scenario

The eavesdropping threat scenario involves an attacker compromising the confidentiality of data in transit. The threat model assumes that the attacker is able to gain access to one of the two channels used for communications.

Figure 2 shows a flowchart that models the attacker's possible courses of action. Note that, in order to be successful, the attacker must locate one of the two channels and properly analyze the data.

Table 1 presents three mitigation strategies based on the threat model along with their outcomes. The first mitigation strategy enables the attacker to obtain only the portion of the data that is sent over the compromised channel. Whether or not the data accessed is adequate to accomplish the attacker's

*Table 1.* Eavesdropping attack mitigation strategies.

| | | |
|---|---|---|
| **Strategy 1** | **Mitigation** | Split the data between the two channels. |
| | **Outcome** | Eavesdropper is limited to the collection of partial data (only the data sent over the compromised channel). |
| **Strategy 2** | **Mitigation** | Send no data over the compromised channel. |
| | **Outcome** | Eavesdropper has no data, but the eavesdropper may become suspicious and search for other frequencies because no data is being sent. The data transfer rate is cut in half. |
| **Strategy 3** | **Mitigation** | Send the data over the uncompromised channel. Send faux data over the compromised channel. |
| | **Outcome** | Eavesdropper only has worthless or misleading data. The data transfer rate is cut in half. |

goal depends on the type of data being sent and the percentage of data that traverses the compromised path. This mitigation strategy enables the sender and receiver to tailor the volume of revealed data to meet their security posture. For example, if confidentiality is not a priority, the communicating entities may choose to send half the data over the compromised channel in order to obtain the best data transfer rate.

The second mitigation strategy sends no data over the compromised channel. It is appropriate when confidentiality is of upmost importance. The strategy defeats the attacker by sending no data via the compromised channel, but the absence of data flow in the compromised channel could alert the attacker to the mitigation strategy. Additionally, the data transfer rate is cut in half.

The third strategy sends faux data over the compromised channel. The attacker does not know about the mitigation and is misled; however, the data transfer rate is cut in half.

The three eavesdropping mitigation strategies are formalized as the two-channel data transmission policies shown in Table 2. In the example, Channel A is assumed to be secure whereas Channel B is assumed to be compromised.

## 3.3 Data Modification Scenario

The second threat scenario involves data modification, where the attacker changes a portion of the data in transit. This attack compromises data integrity.

Figure 3 shows a flowchart that models the attacker's possible courses of action. The attacker has to modify the data successfully and ensure that the recipient does not discover that the data has been modified. If the recipient notices that the data has been changed, the sender could be requested to retransmit the data over the known secure channel.

Leveraging this fact, a mitigation strategy is formulated that enables the receiver to detect data modification. This is accomplished by computing a

*Table 2.* Eavesdropping attack policies (Channel B is compromised).

| Policy | Channel | Data Sent |
|---|---|---|
| 1 | A | 50% of data per packet |
| | B | 50% of data per packet |
| 2 | A | 100% |
| | B | 0% |
| 3 | A | 100% of actual data |
| | B | Random data (0% real data) |

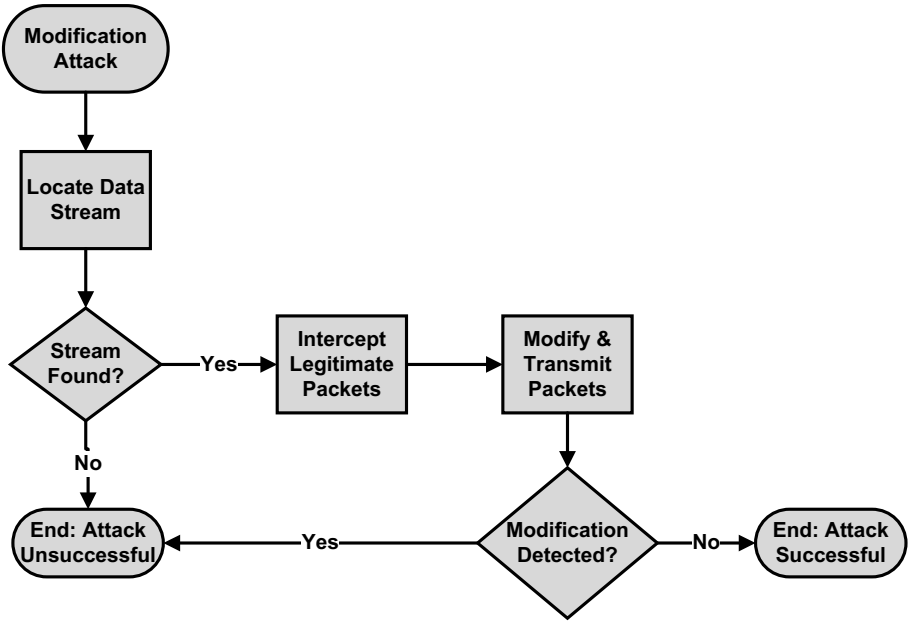


*Figure 3.* Data modification attack.

cyclic redundancy code (CRC) at the sender and verifying the code at the receiver to ensure that the data has not been modified. A sufficiently strong CRC could enable any amount of data modification to be detected. While this may not be the most efficient method, it is suitable to demonstrate the concept [3].

Consider the case where 50% of the data is sent over each channel and a CRC is computed for each packet of data before it is split between the two channels. The CRC itself is split into two parts with each part sent over a different channel. Note that an additional CRC would be computed on the data sent

*Table 3.* Data modification attack mitigation strategies.

| | | |
|---|---|---|
| **Strategy 1** | **Mitigation** | Compute a CRC for the data on one channel to detect if it has been modified. If the attack is detected, cease data transfer over the compromised channel. Transfer all the data over the secure channel. |
| | **Outcome** | Attacker is unable to modify the data without being detected. However, the attacker may become suspicious if data transfer is ceased. The data transfer rate is reduced because only one channel is used. |
| **Strategy 2** | **Mitigation** | Compute a CRC for the data on one channel to detect if it has been modified. If the attack is detected, transfer only faux data over the compromised channel. Transfer all the data over the secure channel. |
| | **Outcome** | Attacker is unable to modify the data without being detected and is unaware that the attack has been detected if data continues to be sent over the compromised channel. The data transfer rate is reduced because only one channel is used. |

over each channel to protect the data being transmitted. Also, the attacker who has access to only one channel cannot generate the correct CRC for the modified data sent over the compromised channel. This is because the other half of the data is unknown to the attacker. As a result, any data modification would be detected when the receiver combines the data and CRC halves and checks the combined CRC. Table 3 presents the two mitigation strategies along with their outcomes.

The two mitigation strategies for data modification are formalized as the two-channel data transmission policies shown in Table 4.

## 3.4 Packet Structure Development

In order to implement the five two-channel policies introduced above, it is necessary to design a packet structure that incorporates the data splitting and CRC schemes. Table 5 shows a proof-of-concept two-channel packet structure.

The 26-bit packet structure incorporates the following five fields:

- **Policy:** This three-bit field specifies the policy used to send the packet. The policy numbers (1 through 5) correspond to the five policies presented in Sections 3.2 and 3.3. For example, a `101` in the field denotes Policy 5. The receiver uses this field to ensure that the packets sent over the two channels have matching policy numbers before processing them.

*Table 4.* Data modification attack policies (Channel B is compromised).

| | Channel | Data Sent |
|---|---|---|
| **Policy 4** | A | 50% of the data per packet + CRC → Switch to 100% of the data after unauthorized data modification is detected. |
| | B | 50% of the data per packet + CRC → Switch to 0% of the data after unauthorized data modification is detected. |
| **Policy 5** | A | 50% of the data per packet + CRC → Switch to 100% of the data after unauthorized data modification is detected. |
| | B | 50% of the data per packet + CRC → Switch to 100% faux data after unauthorized data modification is detected. |

*Table 5.* Proof-of-concept two-channel packet structure.

| | Bits 0-2 | Bits 3-10 | Bits 11-14 | Bits 15-17 | Bits 18-25 |
|---|---|---|---|---|---|
| **Channel A** | Policy | MessageA | CRC-DataA | Packet# | CRC-Msg1 |
| **Channel B** | Policy | MessageB | CRC-DataB | Packet# | CRC-Msg2 |

- **MessageX:** This eight-bit field contains the data bits. The first eight bits are loaded into the MessageA field while the second eight bits are loaded into the MessageB field.

- **CRC-DataX:** This four-bit field contains the data CRC required by Policy 4 and Policy 5 in order to detect data modification attacks. It is formed by generating an eight-bit code from the sixteen bits of data (MessageA + MessageB). Then, the first four-bits of the eight-bit data CRC are loaded into the CRC-DataA field and the second four-bits are loaded into the CRC-DataB field.

- **Packet#:** This three-bit field records the packet number. Packets sent over one channel have a matching packet with the identical packet number sent over the other channel. The packet numbers help ensure that the correct packets are processed together by the receiver.

- **CRC-Msg#:** This eight-bit field is used for error detection during message transmission. The eight-bit CRC for a message is generated using the entire eighteen bits of the message, which is verified by the receiver.

## 4. Conclusions

Maintaining confidentiality and trust for wireless data transmissions are vital to sensor networks used in critical infrastructure assets. However, remote sensors are often power-limited, bandwidth-constrained or too rudimentary to accommodate the power and latency overhead of robust encryption and decryption operations. The two-channel communications methodology presented in this chapter splits the transmitted data over two wireless channels to provide acceptable levels of data confidentiality and/or integrity for non-encrypted remote sensor networks.

The threat scenarios considered involve an attacker gaining man-in-the-middle access to one of the two communications channels to eavesdrop on or modify data in transit. To combat these threats, five data splitting policies are presented that detect and adapt to the attacks while providing varying levels of data security.

Future research will attempt to create additional two-channel policies that can combat other threat scenarios such as denial-of-service attacks and spoofing attacks [2]. These policies will be simulated in software or implemented in hardware to evaluate their effectiveness in real-time applications. Additionally, a measurement and comparison framework will be constructed to gauge the effectiveness of the policies and corresponding packet structures in combating data threats.

Note that the views expressed in this chapter are those of the authors and do not reflect the official policy or position of the U.S. Air Force, U.S. Department of Defense or U.S. Government.

## References

[1] R. Beaulieu, S. Treatman-Clark, D. Shors, B. Weeks, J. Smith and L. Wingers, The SIMON and SPECK lightweight block ciphers, *Proceedings of the Fifty-Second ACM/EDAC/IEEE Design Automation Conference*, 2015.

[2] H. Kalita and A. Kar, Wireless sensor network security analysis, *International Journal of Next-Generation Networks*, vol. 1(1), pp. 1–10, 2009.

[3] P. Koopman and T. Chakravarty, Cyclic redundancy code (CRC) polynomial selection for embedded networks, *Proceedings of the International Conference on Dependable Systems and Networks*, pp. 145–154, 2004.

[4] T. Nie, L. Zhou and Z. Lu, Power evaluation methods for data encryption algorithms, *IET Software*, vol. 8(1), pp. 12–18, 2014.

[5] G. Padmavathi and D. Shanmugapriya, A survey of attacks, security mechanisms and challenges in wireless sensor networks, *International Journal of Computer Science and Information Security*, vol. 4(1-2), paper no. 20070913, 2009.

[6] Y. Shiu, S. Chang, H. Wu, S. Huang and H. Chen, Physical layer security in wireless networks: A tutorial, *IEEE Wireless Communications*, vol. 18(2), pp. 66–74, 2011.

[7] F. Zhang, R. Dojen and T. Coffey, Comparative performance and energy consumption analysis of different AES implementations on a wireless sensor network node, *International Journal of Sensor Networks*, vol. 10(4), pp. 192–201, 2011.