Security issues in wireless sensor networks

Manoj Kumar
B70629
Topic Supervisor - Vitaly Skachek
Research Seminar in Cryptography(MTAT.07.022)

kumarman@ut.ee

Abstract

Wireless sensor network consists of densely populated nodes connected to one another. In a typical sensor network environment, sensor nodes communicate with one or more base stations. Wireless sensor network is widely used in different areas such as agriculture, healthcare, defense, and other research areas. These areas differ in term of their respective security requirements. Areas such as agriculture demand less security, whereas defense and healthcare require more security. Resource constraints of sensor nodes make it complicated to implement classical security approaches in a wireless sensor network. This report overviews the existing literature on security issues in a wireless sensor network. In this report, security requirements are defined in a typical sensor network. Possible attacks are shown on different communication layers along with their mitigations. The feasibility of cryptographic measures is also examined in order to enforce security in the wireless sensor network. We discuss secure key exchange techniques to exchange cryptographic keys between sensor nodes and the base station. Additionally, The area of adaptive security is touched before concluding this report.

KEYWORDS: Wireless sensor network, Cryptography, Security
1 Introduction

A wireless sensor network is the collection of sensor nodes which connect to each other using wireless media. Distributed and dynamic in nature of wireless sensor network allows nodes to form spontaneous topologies. Sensor nodes are often deployed in different and challenging geographical conditions. Sensor nodes vary in the size and cost depending upon the usages and criticality. Wireless sensor networks are designed to be the fault tolerant and resilience in order to deal with the node failure. Most of the modern sensor networks are scalable in nature. Sensor networks are used in the various real-world application. Some of the applications are mentioned below.

- Wireless sensor network is widely used in defense applications such as detection of intrusion or explosives.
- Doctors use sensors to get the updates on patient health and receive patient data such as blood pressure.
- An agriculture based application of the wireless sensor network is to monitor the irrigation requirements in the fields.
- Sensor nodes can detect fire in the woods.
- Sensors are used to detect the pollution in the water and air.
- In a typical data center environment, temperature is monitored using wireless sensors.

Aforementioned applications show the versatile use of wireless sensor network. With the criticality of the sensor application, it is also critical to ensure the physical security of sensor node from any potential adversary and establish the secure communication between sensor nodes and the base station. However, before moving to security requirements and implementations, it is important to understand the architecture of a sensor node and constraints associated with it. The rest of the report is struc-
tured as follows.

Section 2 describes the components of a sensor node. Section 3 gives an overview of possible attacks on different OSI layers. We also describe mitigations to these attacks in this section. In section 4, we discuss the cryptographic protocols used in wireless sensor network. Section 5 shows various key management techniques for wireless sensor networks. Section 6 focuses on the implementation of adaptive security. Finally, we conclude the report in section 7.

## 2 Sensor node

Figure 1 shows the components of a sensor node. A typical sensor node in-

![Sensor node architecture](image)

cludes four primary components, a sensing unit, a processing unit, transmission unit, and power unit.

**Sensing unit** - Sensing unit includes one or more sensor components and an analog to digital converter or ADC. The sensor generates the data, which is converted to digital signals by ADC.

**Processing unit** - Processing unit consists of a processor and small storage. The processor processes the information obtained from sensing unit.

**Transmission unit** - This unit contains transceiver and responsible for the transfer of data to the base station and other nodes.

**Power Unit** - Power unit is responsible for providing power to the node and is highly critical for the life of a sensor node. A power component can be a static battery or rechargeable source of power such as solar power based batteries.

In addition to aforementioned, sensor node can also include a position
finding system to detect the location and a mobilizer unit for movements. Wireless sensor node architecture and network topologies enforce several limitations upon the sensor network. Frequency ranges used by wireless sensor networks to exchange data are limited. Sensor nodes have limited memory and processing capability. Sensor node’s life depends upon the life of the power source. Unfortunately, in wireless sensor network, power resources are also limited. Sensor nodes are often deployed in harsh environment. Tough physical conditions lead to failure of a node and sudden topological changes in the sensor network. These constraints make it infeasible to use computationally expensive security algorithms in wireless sensor network.

3 Attacks on wireless sensor network

Communication among sensor nodes and the base station can be divided into various communication layers[1]. These layers have different functionalities and are prone to different attacks. Functionalities and attacks on communication layers are discussed below. Figure 2 shows a summary of attacks and the mitigations for the attacks.

<table>
<thead>
<tr>
<th>Layer</th>
<th>Attacks</th>
<th>Security Measures</th>
</tr>
</thead>
<tbody>
<tr>
<td>Transport</td>
<td>Flooding, Desynchronization</td>
<td>Client puzzles, Authentication</td>
</tr>
<tr>
<td>Network</td>
<td>Spooled, Altered or replayed routing information, Selective forwarding, Sybil, Wormholes, False flood attacks, Acknowledgement spoofing</td>
<td>Eugenic Filtering, Authentication, Monitoring, Redundancy, Probing</td>
</tr>
<tr>
<td>Link</td>
<td>Collision, Exhaustion, Unfairness</td>
<td>Error-correcting codes, Rate limitation, Small frames</td>
</tr>
<tr>
<td>Physical</td>
<td>Jamming, Tampering</td>
<td>Spread-spectrum, Tamper-proofing, Poorly messages, Hiding</td>
</tr>
</tbody>
</table>

Figure 2. Attacks and mitigations

3.1 Physical Layer

The physical layer deals with the node hardware and wireless media signals. It is responsible for the selection of frequency, modulation, and demodulation. Physical layer attacks on the wireless sensor network include Jamming and Tampering. In Jamming, the adversary tried to disrupt the
carrier frequency. The jamming attack can be mitigated with the frequency hopping spread spectrum. Frequency hopping spread spectrum[2] allows the node to switch carrier frequencies so that adversary does not get a specific frequency to jam. Wireless sensor nodes are often placed in open geographical areas and can be captured physically by the adversary. An adversary can perform tampering attack by changing the configuration such as cryptographic keys of the node. The solution to tampering attack is the use of tamper proof sensor nodes. However, It increases the cost of building the network as tamper proof nodes are expensive.

3.2 Link layer

Link layer is the second layer of OSI protocol. It is responsible for multiplexing, resource allocation and management, data frame detection, medium access and error correction. Possible attacks on link layer include collision and resource exhaustion. An Adversary transmits to the already in use frequency in order to perform collisions. Collision attack leads to the loss or modification of data. These attacks can be prevented using error correction codes. Error correction codes add computational overhead on the sensor nodes but work well with low-level collisions. Adversary tries to overwhelm the wireless sensor network resources to execute exhaustion attack. This attack can be mitigated enforcing limits on the resource allocation per node.

3.3 Network layer

The network layer is responsible for the routing part among sensor nodes and the base station. Relayed routing, selective forwarding, sinkhole, Sybil, wormholes, and hello-flood attacks are some of the attacks possible on this layer. Adversary tries to spoof or replay the network information to affect the network traffic. Use of message authentication codes[3] is a countermeasure to this attack. In order to invoke selective forwarding, an adversary injects a malicious node inside the wireless sensor network. This node does not forward all received traffic to perform selective forwarding. The defense to this attack is using multiple paths so that adversary is not able to perform selective forwarding for entire traffic. Sinkhole attack is performed by advertising routes with lower cost to attract the traffic towards the compromised node, whereas in Sybil attack, a node can advertise more than one identity. Wormhole attack injects a low la-
tency link within the network to attract the traffic. The solution to defend against wormhole attack is the use of packet leashes. Hello flood attacks try to flood the network path by broadcasting hello packets.

### 3.4 Transport layer

This layer is responsible for management of end to end connections and guaranteed delivery of the packets. Flooding and desynchronization are the attacks possible at this layer. Flooding attacks are invoked by creating embryonic connections. This attack can be mitigated by implementing puzzle solving before establishing any new connection. The puzzle is computationally expensive to solve and slows down adversary’s speed to perform new connection requests. Additionally, an adversary can simply try to disturb existing connections by repeatedly altering the messages. This attack is called desynchronization attack and can be defended by implementing authentication before accepting a message.

Session, presentation and application layers are remaining three layers of OSI model. However, we are not discussing issues on these layers in this report.

### 4 Cryptography in wireless sensor network

Cryptography is used to secure the communication between sensor nodes and the base station. Cryptographic protocols are divided into below two categories in general.

#### 4.1 Symmetric encryption protocols

Symmetric encryption uses the same shared secret key for encryption and decryption of the data. The sender encrypts plain text using a secret key and the receiver uses the same key to decrypt the ciphertext(fig. 3). The secret key is required to be shared over a secure out-of-band medium. In case of more than one sender-receiver pairs, the secret key should be unique for each pair. Advance encryption standard(AES)[5] and triple data standard encryption(3DES)[6] are examples of symmetric encryption techniques. symmetric encryption is comparatively swift than the public key encryption. With the correct secret key, a message can be both encrypted and decrypted by an unauthorized person.
4.2 Asymmetric encryption

Asymmetric encryption or public key encryption uses the private-public key pair for data encryption and decryption. The public key can be communicated widely, while only the owner has the private key. In order to communicate a message using public key encryption, the sender encrypts the data using the public key of the receiver. The receiver then uses its private key to decrypt the ciphertext. A key pair ensures that data encrypted with the public key can only be decrypted using the matching private key. Rivest-Shamir Adleman (RSA)[7] authentication and El-Gamal[8] are relevant examples of public key encryption. (Fig. 4).

Public key protocols such as RSA and ElGamal consume more resources than symmetric protocols. Considering the resource constraints in the wireless sensor nodes, symmetric encryption protocols are preferred over public key encryption protocols. Using Symmetric key encryption scheme
allows sensor nodes to live longer as they consume fewer resources and computationally cheaper than public key encryption protocols. RSA takes more than tens of seconds and thousands of nanojoules to perform simple operations. An adversary can take advantage of this to perform a denial of service attack. In contrast to RSA, elliptic curve cryptography\[10\] or ECC gives the same level of protection with a smaller key size. For example, RSA-1024 is equivalent to ECC-160 whereas security of RSA-2048 can be compared with ECC-224\[11\]. ECC based signature schemes are also cheaper than RSA based signature schemes. It is feasible to use ECC in some resource-rich sensor nodes. However, it is still infeasible to use public key cryptography in the majority of the wireless sensor networks.

5 Key management

Key Management in wireless sensor network is mostly based on symmetric encryption schemes as public key cryptography is not a feasible solution for wireless sensor network. Pairwise key distribution can be performed on the small network as it uses one key for each pair of nodes. However, it is impractical for the larger network as each node has to manage \(N - 1\) keys in an \(N\) node large network. In a typical sensor network, most of the node's communication is with its neighboring nodes and most of the pairwise keys will go unused. Key distribution is categorized into below-described categories\[11\].

5.1 Centralized key management schemes

These schemes have a centralized key distribution entity called key distribution center or KDC. The KDC is entirely responsible for the key management, distribution, and revocation of the keys. Centralized key management schemes are vulnerable to the single point of failures as entire key distribution depends upon the KDC. LKHW scheme \[12\] is an example of centralized key management schemes.

5.2 Distributed key management schemes

Key distribution, management, and revocation functions are divided into different entities under distributed key management schemes. This approach is better as it is not vulnerable to the single point of failure. Most
of the key management schemes for wireless sensor networks come under this category. Localize encryption and authentication protocol or LEAP and random key schemes are some examples of distributed key management schemes.

Key management schemes are further categories into deterministic and probabilistic schemes based on the probability of key sharing.

**Localize encryption and authentication protocol**

LEAP comes under the categories of distributed and deterministic key management schemes. LEAP supports four different keys at each node. The individual key is pre-distributed and shared with the base station. The group key is also pre-distributed and shared by all nodes in the network. The pairwise key is shared by immediate neighbors and use to protect the peer to peer communication between neighboring nodes. Cluster key is used for local broadcast and shared by multiple neighboring nodes in the same network.

**Key generation**

Pairwise and cluster keys between nodes A and B are generated using below approach.

- Each node is loaded with key $K_i$

- A generates master key $K_A = F_{K_I}(A)$

- A initiates neighbor discovery by broadcasting hello messages containing its id. The acknowledgement from neighbors contains their id and authenticated using the master key derived in earlier step
  
  $B \Rightarrow * : A$
  
  $B \Rightarrow A:B, MAC(K_B, A|B)$

- Node A computes the pairwise key with B
  
  $K_{AB} = F_{K_A}(B)$

- B also knows A, $K_B$, can also compute $K_{AB}$
5.3 Key pre-distribution scheme

This approach comes under probabilistic key sharing schemes. Each sensor node has a key ring. The ring has a set of \( K \) keys in the memory. These \( K \) keys are taken randomly from the pool of \( P \) keys. The base station keeps the information of the association of key identifier and node identifier. Each node shares a pairwise key with the base station to ensure safe communication with the base station. Shared key is discovered between nodes using two approaches.

**Broadcasting key id** - Node broadcasts its key id without any encryption. A node with the same id identifies the key id and respond back. This approach is vulnerable as adversary can track the unencrypted key id.

**Challenge response** - Node sends a challenge encrypted with its key id. The node with the same id can decrypt the challenge and solve it. Upon solving the challenge, receiver notify the sender and set up the pairwise key.

Additionally, a path key is established to interact with the nodes which are on the same network but do not share a key.

5.4 Q-composite keying scheme

Q-composite keying scheme uses at least \( Q \) common keys from the shared pool of keys. This approach affects more than one communications in case any key is compromised since keys are shared by multiple pairs of nodes. The key update phase shown in figure 5 is used to enhance the security of key distribution. Sender generates \( N \) random values for \( N \) possible path and perform XOR of the key and all path values before sending it to the receiver. In this way, an adversary cannot identify the key for a particular path.

6 Adaptive security

Adaptive security is the modification to traditional static security approach where security parameters are adjusted and maintained according to the varying situations. Adaptive security uses comparatively week security parameter if conditions are favorable. In contrary, for the insecure environment, strong security parameters are enforced. Adaptive security is critical in the wireless sensor network as it consumes less power and
The worst case of adaptive security is static security where conditions are always insecure and strong security measures are implemented. Adaptive security can be categorized into following categories.

### 6.1 Threat centric

Threat centric approach evaluates the network and defines the severity of threat in the network. Security parameters are adapted according to threat evaluation. This approach uses trust management to modify the security. It establishes a trust value for each node and uses this value to evaluate the threat. Figure 6 shows the trust based approach [13] to adapt the security. Gateway has two paths to reach the another gateway. Both paths have different trust levels. Trust levels are defined on the basis of different approaches. These approaches can include the node's performance, feedback from the peer nodes, own observations, packet drop...
and congestion rates. As we can see, AES-256 is used for less trusted path whereas AES-128 is used for more trusted path.

6.2 Data centric

Data centric approach uses criticality and sensitivity of data to perform the adaptation. Unlike, the threat-centric approach, this approach can be established end to end. A node can host one or more application in the sensor network and have associated security requirements per application. Security gradually decreases based on the remaining energy and workload on each node. Once energy and workload are enhanced, security requirements can be restored back. Figure 7 demonstrates the security adaptation based on data criticality[14]. Node has i configurations for N hosted applications. The total number of possible configurations for all applications is \( N \times i \). In case of less energy and higher workload, the configuration is decreased to i-1 and upgraded to i+1 in opposite scenario.

![Diagram](image)

**Figure 7.** Data centric key adaptation

7 Conclusion

Security is a critical aspect of any network. In wireless sensor network, security is implemented considering the limited availability of resources such as processing power, memory, and battery. Most of the classical network attacks are applicable to the wireless sensor networks as well. However, solutions differ due to node constraints. Most of the implemented cryptography in wireless sensor network is based on symmetric cryptography as public key cryptography is not feasible due to it's computationally expensive nature. Key distribution is heavily based on symmetric key cryptography. Static security is not optimal for wireless sensor network as it consumes unnecessary resources when the network insecure. This is optimized using security adaption based on trust and data criticality.
References


