Security Issues in Wireless Sensor Network

Malik Najmus Saqib[1†]

Department of Cybersecurity, College of Computer Science and Engineering,
University of Jeddah, Jeddah, KSA

Summary
Wireless sensor network has been used in many state-of-the-art applications from home automation to warfare. It has become an unavoidable technology that cannot be ignored for the development of modern sophisticated applications. In current era of rapid technological development where new threats are emerging every day, Wireless Sensor Network (WSN) cannot be deployed without the proper security implementations. But the sensor nodes are equipped with the resource constraint components in term of battery life, memory and communication range. In this paper we have highlighted security issue in Wireless Sensor Network and proposed a security mechanism for secure communication among nodes of Wireless Sensor Network. Various cryptographic algorithms are used to implement the proposed mechanism and compared with respect to time. It is concluded that elliptic cure is most suitable for WSN in term of efficiency and security.

Key words:
Wireless sensor network, security, confidentiality, integrity, authentication, cryptographic algorithm. Time complexity

1. Introduction

A wireless sensor network is system that consists of nodes that communicate with each other through wireless medium. Each node has a measuring, sensing, communicating and computing elements. This provides the functionality to supervisor for observing, reacting and instrument to the environment [1]. The supervisor of such network may belong to governmental department, civilian, industrial or commercial setup.

Wireless network systems are one of the vital technologies nowadays. In past few decades it faces major development. Wireless Sensor Networks (WSN) become the interest of many applications that include collecting and processing data, monitoring and surveillance, controlling and activation, and medical telemetry [2]. WSNs are equipped with advanced low-cost communication technologies and hardware with which the development of tiny nodes (device) is possible at exceptionally lower rate than the available traditional sensors [3]. Many research and application in the field of ad-hoc network are explored due to development of WSNs. Although WSNs consist of many small nodes that are low in memory, energy, computational and transmission coverage but they have been proved to be one of the possible versatile, low cost tools that is used for controlling, monitoring, searching and etc for wide range of applications [3].

A diversity of sensors may be attached with the nodes of Wireless Sensor Networks to monitor the properties from the environment. These sensors include but not limited to magnetic, chemical, mechanical, optical and biological sensors. These sensor nodes are deployed at the location which is difficult to access physically and equipped with the radio for the wireless communication with the base station for the transfer of gathered data from environment. The base station is typically a resourceful node in term of energy, memory and transmission range. It can be a personal handheld device or laptop that plays the role of access point to the infrastructure. The main power source of sensor node is battery. It is possible to provide the secondary power source from environment e.g. solar panels or wind turbine to the node depending on the circumstance of the environment where the sensor are deployed.

Wireless sensor technology has been affected with the rapid development modern threats that may compromise the communication of nodes in Wireless Sensor Network. Nowadays it is almost impossible to deploy a wireless sensor network without security measures. The security measures are mostly available in term of cryptographic algorithms. Cryptographic algorithms are considered most secure till now, but these algorithms take much system resources in terms of memory, time and power. In this paper we have highlighted security issues in Wireless sensor network. We have proposed a mechanism for the secure communication among nodes in wireless sensor network. This work also provides a comparison among state-of-the-art cryptographic algorithm that can be used to for secure communication.

This paper is organized as follow. Section 2 discusses applications of Wireless sensor network. Section 3 provides review of literature. Section 4 proposes the secure communication mechanism. Section 5 provide the details of experiment performed and results. Section 6 conclude the paper.

Manuscript received July 7, 2020
Manuscript revised July 20, 2020

2. Application of Wireless Sensor Network

WSN provide low cost solution and can be installed in the environment where human cannot reached/worked. That why WSN are poplar and used in many applications [4]. In the following we have discussed various application of wireless sensor network [1].

2.1 Home Automation

The use of wireless sensor network in home control application provides safety, control, convenience and conversation [5]. Following are the few examples

- It allows flexible management of Heating, ventilation and air conditioning (HVAC) HVAC from anywhere in the home.
- It is used for the communication of home control system without wires
- It is used to acquire precise detailed usage of utilities like water gas and electricity
- It is used to achieve optimal consumption of nature resources
- It is used for the detection of abnormal event via automatic alarm or notifications.

2.2 Building Automation

Wireless sensor network can be used to accomplish the wireless lightening control system. Specifically, ZigBee technology is preferable to be used for this purpose. Lightening control system includes customizable and controllable lightening schemes and saving power on bright days. Energy is the big expense for any hotel. Wireless sensor network and ZigBee technologies can be used for the energy management in big Hotels e.g. making sure that empty rooms are not cooled by the centralized HAVC system. Assets management is another application of wireless sensor network for example wireless sensor can be attached to each container to monitor its location. To ensure security through on ship or on truck tamper detection sensor provides a decent solution. Before the time when ship is dock at the port sensor data is known, thus provide faster container processing.

2.3 Industrial Automation

Wireless Sensor nodes provide efficiency, accuracy, communication, safety and control in various industrial automation applications in the following manner

- Sensor nodes applications are helpful in term of safety in existing process of manufacturing and control systems.
- Sensor nodes applications can monitor the critical components of asset continuously.
- Sensor nodes applications is a major contributing factor in optimizing the manufacturing process to reduce the energy costs
- The equipment that is performing poorly and operations that are inefficient can be identified via sensor nodes applications

By deploying the sensor nodes applications, the user interference will be reduced to collect data from the remote sensor

2.4 Medical Applications

Wireless sensor network can be used to monitor patient especially elderly and critical once. It can further be used for diagnostics, animal movements in specific region and internal process. The check on medicine administration in medical centers and doctor monitoring can be done using wireless sensor network [7].

A wide range of medical center and hospital management are using the applications of wireless sensor network technologies in the wide spectrum of medical applications that includes hospital emergency, rehabilitation of patient and disaster response. Wireless sensor network are very useful for the monitoring of chronic and elderly people at home by providing the facilitation of long term care and analysis. This will obviously reduce the time of patient he will stay in hospital. Wireless sensor node help in the collection of long-term medical information of patients from various parts that will populate database of clinical data. This will enable the doctors and physician to studies and perform research on the data.

2.5 Disaster relief operation

Nowadays to acquire the information for post disaster operations the wireless sensor network has been used widely [6]. The sensor node can be dropped through a plane or helicopter in area that is reported to have some kind of disaster such as wildfire, damage are as a result of earthquake and flooded area and that is difficult to access physically. In the region of fire, a wireless sensor network is used to construct a temperature map by acquiring the sensed information from each node. This temperature map is used to determine the appropriate techniques and procedures to extinguishing the fire.

2.6 Military Application

Due to self and rapidly organizing nature, wireless sensor network can be used for monitoring and sensing the environment and detection of hostile movement [8]. The decision in the battlefield e.g. in case more ammunitions,

forces or equipment is required can be performed based upon the surveillance of battlefield done though the wireless sensor network. Wireless senor nodes can be spread out to detect any nuclear, biological and chemical attacks. An interesting example is the sniper detection system. This system uses acoustic sensor for detection of incoming firing and to estimate the sniper's position by processing the audio sounds detected from the microphone of sensor nodes.
In [9] an antitank landmines system is described supported by a network. Each node in this system monitors the state of its neighbor nodes. Nodes senses for any possible threats and response to those threats itself by moving further. Distributed self-sufficient audio location system and accelerometer sensor are the bases of sensing. The direction of the next generation Self-healing land mine system is provided in [10].

2.7 Environmental Applications

Environmental monitoring can be efficiently and accurate done in real time by using a wireless sensor network. But environment monitoring involves many factors that must be address while deployment for example harsh weather conditions. Such factor effectively reduces the performance of wireless sensor network. Sensor Scope [11] is an interdisciplinary work that successfully deploy sensor network in real world applications under the rough conditions of environment.
Wireless sensor network can be used to track movement of living things for example birds, animal and humans and safe those movement pattern for future use. Wireless sensor network can be used in precision agriculture and irrigation e.g. sensor can be deployed in the field under soil to determine the moisture, temperature and level of water. Sensor node equipped with sensor can be used to monitor atmosphere context, earth and soil. They can be used in detection of fire, flood, monitoring chemical and biological process, earthquakes etc.

3. Threat Model

In a common sophisticated communication model of Wireless Sensor Network there are sensing nodes installed in sensing areas. These sensing nodes collect the data from that area and transmit it to the sink node. Sink node collects the data from various sensing nodes and transmit it to the central control over the Internet.
Figure 1 shows the threat model for a general wireless sensor network. It consists of a sensor node that collects the data from the environment and pass it to sink node. Sink node process that data send it to the central control over the Internet. Sensing nodes has relatively low computational resources and power as compare to the sink node.
The attack can be active or passive for the communication between the sensing node and sink node and between sink node and control node. Passively, the attacker can collect the encrypted message and can do the traffic analysis later. As active attacker the attacker can perform the following

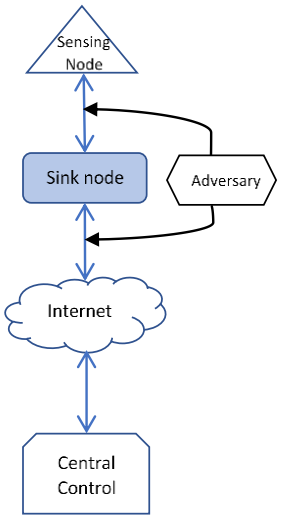

Fig 1: Threat model in common Wireless Sensor Network

a. Can manipulate the data that is transmitted between sensing node and sink node or between the sink node and control node.
b. It can masquerade as one of the sensing node and send false information to sink node.
c. Can send false message to sensing node in order to drain it battery
d. Can read the information that transmitted between sensing node, sink node and central control.

4. Security Requirements

In this section we discuss the security requirements that are desirable in sophisticated Wireless Sensor Network.

4.1 Confidentiality

The data that is sensed from the environment by sensor node and then transmit to the sink node need to be confidential. So that any adversary may not be able to read the data pass between sensing nodes and sink node.
Similarly, the information that is transmitted between the sink node and the central control over the Internet need to be confidential. Both communications can be confidential

by using appropriate encryption algorithms. Such algorithms must consider the low computational resource of sensing nodes.

4.2 Integrity

Besides making the transmission confidential it is also desirable that any changes in the transmission accidental or by adversary should be detectable at the destination node. It is possible that an adversary may not be able to understand the communication as it is encrypted but it can change some bits randomly. Here, the intention of adversary is just to make the communication corrupted without understanding.

4.3 Authentication

Before sink node accept data from the sensing node it must authenticate that the data comes from the legitimate sensing node. An adversary can impersonate as a sensing node and can send false data to sink node. Sensing node make sure not to accept such data from impersonate node. Such data if accepted may result in false information that can lead to wrong decisions.
It is possible to assign the authentication identifier to the sensing devices at the installation time. This identifier is not known to the attacker as it is transmitted in encrypted message.

5. Proposed Mechanism

This section proposes a mechanism of the messages that are transmitted between the sensing node and the sink node. Also, the message between the sink node to the central control node. Elliptic curve cryptography is used in the proposed secure communication. Other famous cryptographic algorithms like Advanced Encryption Standard and RSA are not used as these algorithms are proven to be not good for resource limited devices like sensing nodes. While Elliptic curve cryptography is used for such devices to achieve security requirements.
Format of the message:
The messages that are transmitted between the sensing nodes and the sink node contains the data (sensed from environment) and the identity of the node.

$$ID_{Se} \,||\, Data \text{ ------- } (1)$$

IDSe is the id of the sensing node. The ID of the sensing node and Data is concatenated (||) transmitted as a single message securely. Similarly, sink node send the same kind of message containing its ID (IDSi) and Data/Information to the central control.
Elliptic curve cryptography is used to secure the messages between sink node and sensing node. There two global parameters in Elliptic curve cryptography, which are shared among the sensing nodes and the sink node in a single cluster. These parameters are G and n. G is called the base point of the elliptic curve and n is sufficiently large number. In the following the elliptic curve cryptography process of encryption and decryption [12] is described for the wireless sensor network.
Elliptic curve cryptography is a public key algorithm. That is each entity (sensing nodes and sink node) contains a public and private key. So, the first process is to generate the public and private key pair of each node. For that each node select e and t.

e: a random number between 1 to *n*-1

t: is a point on curve

$$U = e * p$$

At the end each node calculates U as shown above. Now U is the public key and e is the private key of that node. In this way each sensing and sink node has its own public and private key.
After generating the public and private key pair each sensing node can encrypt the message that it sends to sink node as follows
The first step in encryption process is that the sensing node generates a random key k_R ($1 < k_R < n-1$). Then it starts encrypting the message

$$X_{Se} = k_R * t$$

$$Y_{Se} = (ID_{Se} \,||\, Data) + (k_R * U_{Si}) \quad (2)$$

The above X_{Se} and Y_{Se} are the two encrypted messages generated by the sensing node. ID_{Se} || Data are the identity and data of that sensing node. U_{Si} is the public key of sink node.
Similarly, when the sink node wants to send message to controller it will generate the following encrypted messages.

$$X_{Si} = k_R * t$$

$$Y_{Si} = (ID_{Si} \,||\, Data) + (k_R * U_{CC}) \quad (3)$$

X_{Si} and Y_{Si} are the two encrypted messages generated by the sink node. ID_{Si} || Data are the identity and data of that sink node. U_{CC} is the public key of sink node.
The sink node receives the following encrypted messages from sensing node

$$X_{Se}, Y_{Se}$$

To decrypt these messages, sink node perform the following decryption process

$$(ID_{Se} \,||\, Data) = Y_{Se} - e_{Si} * X_{Se} \quad (4)$$

e_{Si} is the private key of the sink node. See Eq (2) where public key of sink node (U_{Si}) is used in encrypting (ID_{Si} || Data).
In the same way, the central control after receiving the encrypted messages (X_{Si} , Y_{Si}) from sink node decrypt them in the following way

$$(ID_{Si} \| Data) = Y_{Si} - e_{CC} * X_{Si}$$

e_{CC} is the private key of central control.
Signature creation process [13] is perform by each node (sensing or sink). When sensing node send a message to sink node, it performs the process of signature creation on message. Following are the steps signature creation process that a sensing node perform each time when it sends a message to sink node.

i. Hash of the message (Eq. 1) is calculated
$H = Hash\ (ID_{Se} \| Data)$

ii. Generates a random key k_R ($1 < k_R < n-1$)

iii. Compute two points on the Elliptic cure
$$(x, y) = k_R * G$$

iv. Calculate l = x % n and if l is 0 then repeat from step 2 by generating another random key

v. Calculate $m = k_R^{-1} (H_{lb} + l * e_{Si})\ mode\ n$. If m is 0 then repeat from step 2 by generating another random key.
e_{Si} is the private key of sensing node. H_{lb} are the left most bits of hash H.

vi. (l, m) is the signature on message $(ID_{Se} \| Data)$

Now the sensing node send the encrypted message along with the generated signature as shown below

$$X_{Se} \| Y_{Se} \| l \| m \quad (5)$$

Signature verification process [13] is performed by receiving node. The message in equation (5) is received by the sink node. Sink node performed the signature verification process. First sink node decrypts the message and get the plaintext message (IDSe || Data) as shown in equation (4). Then it performs the signature verification as shown below

i. Hash of the message (Eq. 1) is calculated
$H = Hash\ (ID_{Se} \| Data)$

ii. Calculate $p = m^{-1} \% n$

iii. Calculate $q_1 = (H_{lb} * p) \% n$
$$q_2 = (l * p) \% n$$

H_{lb} are the left most bits of hash H generated in step (i).

iv. Compute two points on the curse a1 and b1 as follow
$$(a_1, b_1) = q_1 * G + q_2 * U_{Si}$$
U_{Si} is the public key of Sink node

v. When the signature part (l) in the received message is equal to the $a1$ point computed above then the signature considered to be valid and that the message is not change during transmission.

There are three main desirable security requirements that are discussed in section 4. The confidentiality is achieved by encrypting and decrypting the messages. While integrity and authentication are achieved by signature.

6. Experiment

We have performed the experiment of encryption and decryption of data of various sizes by using three famous cryptographic algorithms. These are Advanced Encryption Standard (AES), Rivest–Shamir–Adleman (RSA) and Elliptic-curve cryptography (ECC). The platform that is used to perform experiments is Intel (R) core i7 – 3740QM, 2.7 GHz CPU and 8GB RAM. The experiments are performed to proof the concept that ECC is more efficient than AES and RSA. The key size of AES algorithms is 256, RSA is 2048 and ECC is 256 bits. Experiments are performed only with these key sizes as these key sizes are considered to be safe nowadays.

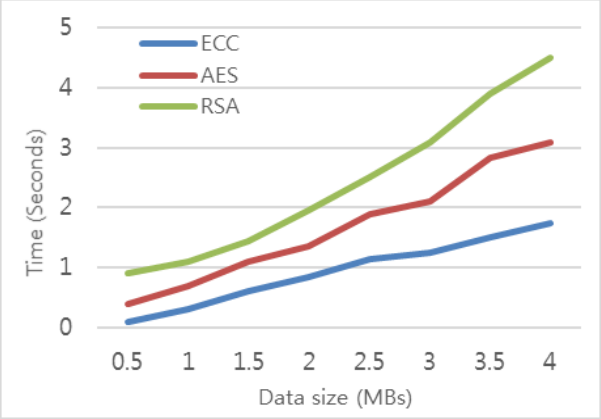

Fig. 2 Comparison of En-/Decryption time of ECC, AES and RSA

Fig 2 shows the encryption time for the three popular algorithms AES, RSA and ECC. The graph shows that RSA take more time than ECC and AES. In this experiment we did not include the key distribution time for AES and key generation time for RSA and ECC. The RSA curve shows the trend that as the size of data become

large the time of encryption grow fast as compare to the AES and ECC.

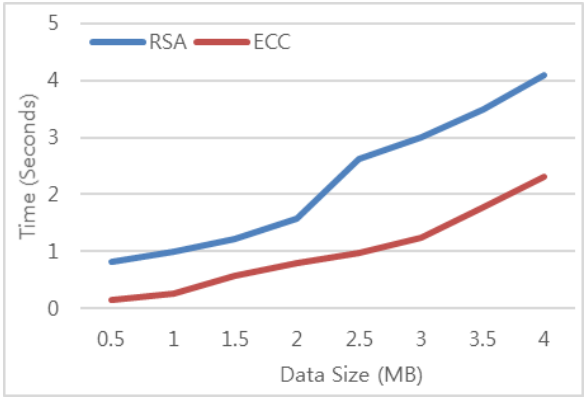

Fig. 3 Signature creations and verification time for RSA and ECC

Fig 3 shows the signature creations and verification time for the RSA and ECC. It is clear from the graph that ECC is more efficient as compare to RSA.

Moreover, the authentication is achieved in RSA and ECC algorithms by creating signature. This process also provides integrity of data that is if data is modified during transmission then the signature verification process is failed. If signature verification process is successful, then it means that data is not changed during transmission and that the data is sent by a legitimate sensor node.

7. Conclusion

Wireless sensors are used in many sophisticated applications nowadays. It is important to make the communication of the sensor node and sink node secure. This research work presented a generalized threat model for Wireless Sensor Network. It identifies the security requirement that are desirable for commonly used WSNs. We have performed experiments by encrypting and decrypting data with various popular cryptographic algorithms like AES, RSA and ECC. It is concluded that ECC performs best in term of time complexity in encryption decryption and signature creation and verification process.

References

[1] K. Sohraby et. al. Wireless Sensor Network Technology, Protocols and Applications, Willey, 2007

[2] Elahi, Gschwender, ZigBee Wireless Sensor and Control Network, Pearson 2010

[3] J. Yick, B. Mukherjee, and D. Ghosal. Wireless sensor network survey. Journal of Computer Networks, Volume 52(Number 12):2292-2330, 2008.

[4] A. Mainwaring, et. al. Wireless sensor networks for habitat monitoring. 1st ACM international workshop on Wireless sensor networks and applications, pages 88_97. ACM, 2002

[5] J. Jin, J. Jin, Y. Wang, K. Zhao, and J. Hu. Development of Remote-Controlled Home Automation System with Wireless Sensor Network. 5th IEEE International Symposium on Embedded Computing, 2008. SEC'08, pages 169_173, 2008.

[6] X. Wang, M. Liu, and B. Liu, Data Evacuation for Wireless Sensor Networks in Disaster Areas, Journal of Advances in Computer Networks, Vol. 1, No. 4, 2013

[7] R. Negra. I. Jemili. A. Belghith, Wireless Body Area Networks: Applications and Technologies, Procedia Computer Science Volume 83, 2016, Pages 1274-1281

[8] Milica Pejanovic Durisic, Zhilbert Tafa, Goran Dimic, A survey of military applications of wireless sensor networks, Mediterranean Conference on Embedded Computing MECO – 2012

[9] William. M. Merrill et al., Defense systems: self-healing land mines, Ch. 18 in Wireless Sensor Networks: A System Perspective, Editors N. Bulusu and S. Jha, Artech House, 2005

[10] William. M. Merril et al., "Dynamic networking and smart sensing enable next-generation land mines," IEEE Pervasive Computing, vol. 3, no. 4, 2004, pp. 84-90

[11] Guillermo Barrenetxea, Franc¸ois Ingelrest, Gunnar Schaefer, and Martin Vetterli, Wireless Sensor Networks for Environmental Monitoring: The Sensor Scope Experience, International Zurich Seminar on Communications March 12-14, 2008

[12] Elliptic Curve Cryptography Algorithm, https://bithin.wordpress.com/2012/02/22/simple-explanation-for-elliptic-curve-cryptography-ecc/, accessed on June 03 2020

[13] Elliptic Curve Digital Signature Algorithm, https://en.wikipedia.org/wiki/Elliptic_Curve_Digital_Signature_Algorithm, accessed on June 04, 2020

Malik Najmus Saqib is working an Assistant Professor in Department of Cybersecurity, Faculty of Computer Science and Engineering, University of Jeddah. He worked as researcher in University of California. He is a member of various technical program committees. He was a expert/resource person in a workshop on "Internet Security: Enhancing Information Exchange Safeguards" organize by COMSATS for 5 years (2011-2015). His research interests include information security and privacy in various state of the art applications and technologies.