IARJSET

ISSN (Online) 2393-8021
ISSN (Print) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

ISO 3297:2007 Certified

Vol. 4, Issue 4, April 2017

Study of Wireless Sensor Networks Security

Marwah A. Mohsin[1], Ashwaq Q. Hameed[2]

University of Information Technology and Communication, Baghdad, Iraq[1]

University of Technology, Baghdad, Iraq[2]

Abstract: Wireless Sensor Networks (WSNs) considered as one of the most exciting and challenging research domains of our time. It have been perceived as extremely advanced and helpful technology in a variety of fields. However, WSNs suffer from many challenges and limitations, including; memory space, bandwidth, power consumption, etc. all of which impose security challenges that make this approach interesting to study. In this study, we present a study of WSNs security challenges by presenting the security requirements, classifying the types of attacks on WSNs (i.g. denial of service (DoS) attack), and illustrating security defence techniques for each type of attack. In addition, we present an Intelligent Home Monitoring System (IHMS), using Received Signal Strength Indicator (RSSI) in WSN that implemented to detect intrusion at home, as an example of the WSNs security.

Keywords: Wireless Sensor Networks, WSNs, Security of Wireless Sensor Networks, IHMS, RSSI.

I. INTRODUCTION

Wireless Sensor Networks (WSN) have been perceived as extremely dynamic and helpful technology in a variety of fields; military target tracking and surveillance, home automation, patient monitoring, e-health tracking and so on. Recent research development in computer and electronics technology, give a chance to generally spread the wireless sensor technology in various domains of life [1,2,3]. WSNs are typically comprise of small sensor nodes which are battery powered and outfitted with data processing capabilities, integrated sensors with short range radio communication [3]. These sensors are economical contrasted with traditional sensors. Besides, the sensor nodes can sense, measure, and aggregate data from the surrounding environment and, rely on some topical decision process, they can transmit the sensed data to the user[4,1].Because of the deployment of WSN in antagonistic and unmonitored environment, these networks are very prone to security attacks than other traditional wired and wireless infrastructure networks [5].

Security permits WSNs to be utilized with certainty and maintains integrity of data. Without security, the utilization of WSN in any application field would led to undesirable results [6]. To design a totally secure WSN, security must be integrated into each node of the network. Any part of a network executed with no security could surly be a point of attack. As a result, the security must invade each part of the design of a wireless sensor network application that would aggregate or distribute critical data; i.e. requiring a high level of security [7].

II. CLASSIFICATION OF SECURITY ATTACKS ON WSNS AND THEIR DEFENCE TECHNIQUES

Denial of Service (DoS)

It is the kind of attack in which tries to transmit redundant data packets to bring about malicious activity in the system. In this DoS, attackers attack a specific node with

redundant data rising the amount of data load on the sensor node restricting the legitimate senders to get to the system. It is purposed to enemy effect the system performance and disrupt the system's capacity to provide services [10].Moreover, various types of DoS attacks are also discussed here:

A. Jamming

In this kind of attack, radio frequencies of sensor nodes are interfered. Jamming source might be sufficiently effective which can easily disrupt the system. An attacker may likewise jam the system with less effective devices which may likewise disturb the system performance by strategically deploying the jammers in the WSN [12].

The most widely recognized protection against jamming attacks is the utilization of spread-spectrum communication. In frequency hopping, a device sends a signal on a frequency for a small period of time, switching to another frequency and iterate. The sender and recipient must be arranged. Direct-sequence distributes the signal over a wide band, utilizing a pseudo-random bit stream. A recipient should know the distributing code to recognize the signal from noise [13].

DOI 10.17148/IARJSET.2017.4401

B. Collision

This type of attack is performed by continuously transmitting messages in the system. Infringement of communication protocol by disturbing the system produces collision attack [12]. This attack is energy efficient for the attacker and effortlessly degrades the system performance. Collision may delay the communication and may modify the messages. Ultimately, mismatched messages at the receiving node need to be retransmitted. If collision happens, energy of sensor nodes get drained soon because of retransmissions and resources such as bandwidth get wastes too [10].

Error correcting codes can be utilized to give some security against devastation of message information. They are appropriate for covering random transmission errors, in which autonomous bits of a message might be flipped. An attacker, however, can always corrupt a bigger number of information than the code can correct. The codes themselves likewise processing and transmission overhead, as the message includes greater redundancy [13].

C. Flooding

In this attack, affected node transmits several connection request to a neighbouring nodes, joining the nodes and making its resources useless. This attack may bring about serious loss of memory and energy resources of sensor nodes in the system [10].

There is a way to deal with reducing the flooding attack which is by asking the clients of services commit significant resources before connections are set up. Client puzzles are one such technique, whereby servers dispense cryptographic puzzles that must be solved by brute-force before connection-related resources on the server are allocated. The difficulty of the puzzles is scalable, so the server can expand the requirements when it constrains it is under attack. In a WSN, this could cause an adversely affects on the many legitimate sensor devices, each of which has restricted resources to commit[13].

D. Wormhole

A wormhole is low latency link between two parts of a system over which an attacker replays network messages. This connection might be set up either by a single node sending messages between two adjacent however generally non-neighbouring nodes or by a couple of nodes in various parts of the system communicating with each other. The last case is similar to sinkhole attack as an attacking node close to the BS can give a one-hop link to that BS by means of the other attacking node in a far part of the network [9]. Figure 2.1 shows the wormhole attack.

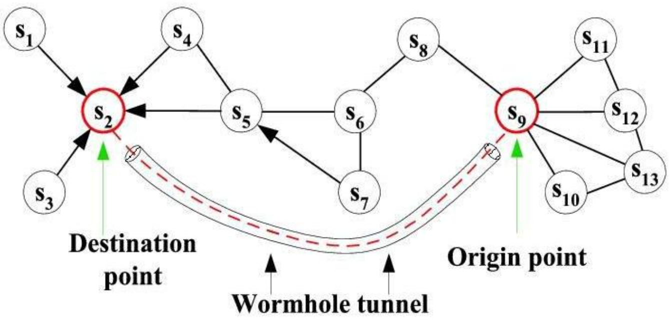

Figure 2.1: Wormhole [8]

A defence mechanism is described based on packet leashes, where the distance that a message may travel in a single hop is constrained. Every message contains a timestamp and the position of the transmitter. The recipient contrasts these and its own position and time to determine whether the maximum transmission range has been surpassed [13].

E. Hello flood

In Hello flood attack Hello packets are deployed with higher transmission power devices (such as PC) to sensor nodes. The node which receive the broadcast messages considers it to be coming from a closest transmitting node. This attack leads to a congestion issue in the system [14].

Checking the bi-directionality of local connections before utilizing them is efficient if the attacker possesses the same reception abilities as the sensor devices. In any case, if the attacker can utilize a critical recipient, it can ultimately convince nodes in the system of its authenticity [13].

F. Sink hole

Sink hole resembles worm hole attack which likewise effects and changes the data in the system. In this attack, malicious node distributes zero-cost route to attract traffic to itself which eventually makes a sink hole. Malicious node is a node close to BS to act as a BS for other nodes as shown in figure 2.2.As a result of the zero-cost route, every node in the system attempt to compete for the unlimited bandwidth which thusly causes contention of resources in the system and that leads to loss of information in the system [15].

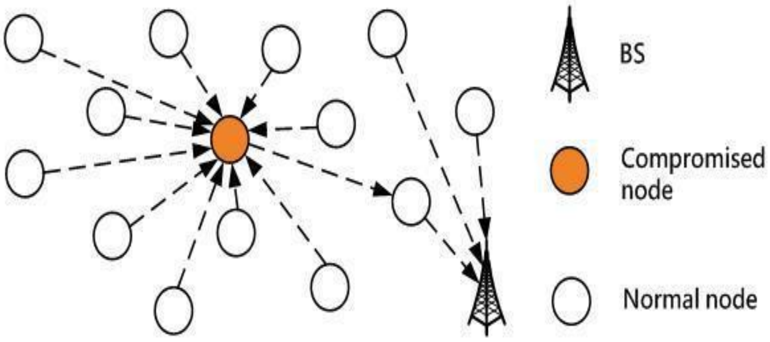

Figure 2.2: Sink hole [15]

One technique used to deal with sink hole attack is to utilize routing algorithms that are renitent to arbitrary configurations, for example, geographic forwarding. Because of that every node creates an autonomous forwarding decision rely on the area of its neighbours, it is not as simple to attract routing to an attacker[13].

G. Sybil

In this kind of attack, malicious node gained many identities, to disrupt the system by causing data redundancy in distributed data storage system. Sybil attack may hurtfully influence the fault tolerance capability of WSN, for example, data aggregation [11]. Figure 2.3 explains the Sybil attack graphically.

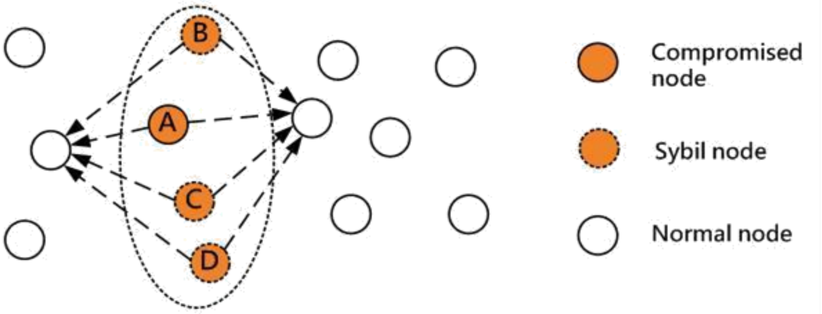

FIGURE 2.3: SYBIL [15]

Since identity fraud is key to the Sybil attack, appropriate authentication is the key for protection. A trusted key server or BS might be utilized to authenticate nodes to each other and bootstrap a shared session key for encoded links. This imposes that each node share a secret key with the key server. In the event that a single key is utilized in a network, compromise of any node in the WSN would fail all authentication [13].

H. Tampering

WSN is typically distribute in outside environments. Nodes in WSN are extremely vulnerable to attacks due to the distribution nature of WSN. This is a kind of physical layer attack which may bring about an irreversible harm to network nodes. Attacker can decrypt cryptographic keys from affected nodes and alter and adjust the codes also [12].
A method to defiance against tampering is to prevent detection of the nodes. Camouflaging the packaging, concealing the device, and utilizing low-probability of intercept (LPI) radio mechanisms are among the probabilities. However, these may all add cost and perplexity to WSN implementation [13].

III. INTELLIGENT HOME MONITORING SYSTEM (IHMS)

This section [16] presents the design of Intelligent Home Monitoring System (IHMS) utilizing Received Signal Strength Indicator (RSSI) in WSN that implemented to detect prospective problems, sending SMS and email to far off home owner to notify the probability of intrusion at home.

A. Components of IHMS

- Software parts consists of small OS and Server on the web to transmit SMS and Email when the system identifies any dangers.
- Hardware parts consists of Tmote as sensor nodes and a tablet or PC with internet connection.

B. Actors of The Proposed System

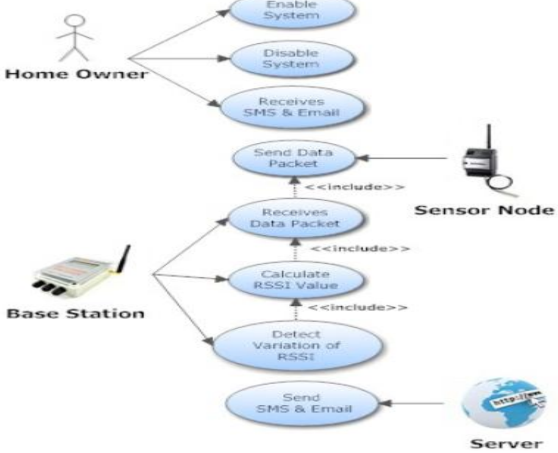

Figure 3.1: Use Case of IHMS [16]

Figure 3.1 presents the use case graph of IHMS. This graph consists of four actors in IHMS and they are introduced as the following:

- **Homeowner**: It is the individual who is in charge of commanding the major actions of the system.
- **Server**: It is the web application that transmits SMS and Email to the Homeowner.
- **Base Station**: It is the tablet (or PC) that receives information from Sensor Motes. At that point the BS determine RSSI rate of received information, and save RSSI values in Data Base, observe difference of RSSI.
- **Sensor Motes**: It is the device that will sense the surrounding environment, then rely on the outcome of sensing will transmits information to BS.

C. Use Case of IHMS

Figure 3.2 explained the state chart diagram of IHMS which illustrates the states of components in a system.

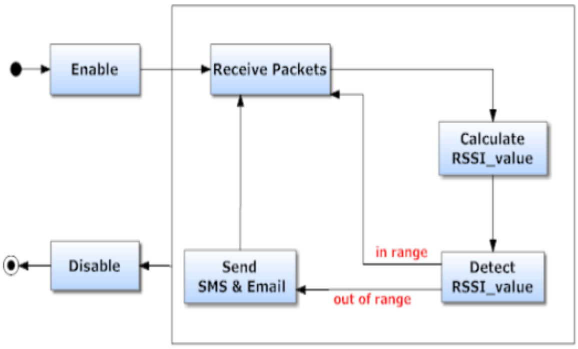

Figure 3.2: State Chart Diagram of IHMS [16]

- **The Enable system use case**

By using this use case the homeowner can turn on the system. This use case begins when homeowner chooses to activate the system. homeowner selects Enable operation of the user interface(UI) by tapping on the Enable button. IHMS run and BS begins receiving information from the Sensor Motes.

- **The Disable system use case**

By using this use case the homeowner can turn off the system. This use case begins when homeowner chooses to deactivate the system. Homeowner selects Disable operation of the UI by tapping on the Disable button. The system transmits SMS to Sensor Motes to go to sleep mode (don't transmit any more information) and leave the application.

- **The Receive SMS and Email use case**

By using this use case the homeowner can receive SMS and email from the server. BS transmits alert to server. The server transmits SMS and Email to homeowner. The homeowner will receive the notification.

- **The send information use case**

In this use case the Sensor Motes can transmit information to BS. homeowner activate the system. Sensor Motes transmit an information after a particular time period to the BS.

- **The Receive information use case**

In this use case BS can receive information from a Sensor Motes.

- **The determine RSSI rates Use Case**

In this use case the BS can determine RSSI rates from received information.

- **The Detect differences of RSSI rates use case**

In this use case BS can distinguish variety in the currently received RSSI rates with already saved RSSI rates in database.

D. Work Mechanism of IHMS

Base Station (BS) gets information from sensor motes. It determines RSSI rates for every received information and save it in its database. At that point BS contrasts received RSSI rates and already saved RSSI rates so as to calculate the differences that must not pass the predefined limit of RSSI rates. In case of that RSSI rates stay in the passable range and the difference is not big from already recorded RSSI rates, then BS continues receiving more information parcels from sensor motes. In case of that the RSSI rate is not in passable range then BS transmits alert to server. The server transmits message to the homeowner for informing the intrusion action at home.

IV. CONCLUSION

- Security in wireless sensor networks has gained more attention in last years.
- When people think like attackers, they will understand better their intentions and this will help them to save their systems better from potential intrusions.
- For IHMS, generate real-time notification via SMS or Email would help to notify the homeowner immediately for any type of attack.
- In these kind of systems we can observe many advantages such as:
- ▪ Easy to use.
- ▪ system installation can be done without fixed infrastructure.
- ▪ Elastic systems; when random situation appears additional workstation is needed.
- ▪ Economical systems.
- ▪ It's accommodative to add new components at any time.
- Ultimately, security is going to play essential role in all domains of WSNs, thus it will continue to be a main research area for the prospective future.

REFERENCES

[1] Jennifer Yick, Biswanath Mukherjee, DipakGhosal *, "Wireless Sensor Network Survey", Computer Networks 52 (2008) 2292–2330.

[2] Rajkumar, Sunitha K R, Dr.H.G.Chandrakanth,"A Survey on Security Attacks in Wireless Sensor Network", International Journal of Engineering Research and Applications (IJERA) Vol. 2, Issue4, July-August (2012), pp.1684-1691 1684.

[3] Araujo, A., Blesa, J., Romero, E., & Villanueva, D. "Security in Cognitive Wireless Sensor Networks. Challenges and Open Problems", EURASIP J WirelCommunNetw, 2012(1), 48.

[4] NeelamSrivastava"Challenges of Next-Generation Wireless Sensor Networks and its Impact on Society", Journal Of Telecommunications, Volume 1, Issue 1, Feb (2010).

[5] Muhammad AhsanRaza, BinishRaza and AnumAftab"Comparative Study Of Security Attacks On Wireless Sensor Networks", International Journal Of Multidisciplinary Sciences And Engineering, Vol. 5, No. 5, May (2014).

[6] Kalpana Sharma1, M.K. Ghose1, Deepak Kumar1, Raja Peeyush Kumar Singh1 and Vikas Kumar Pandey1, "A Comparative Study of Various Security Approaches Used in Wireless Sensor Networks", International Journal of Advanced Science and Technology, Vol. 17, April, (2010).

[7] David Boyle, Thomas Newe, " Securing Wireless Sensor Networks: Security Architectures", JOURNAL OF NETWORKS, VOL. 3, NO. 1, JANUARY (2008).

[8] Arya, R. & Sharma, S. ,"Optimization Approach for Energy Minimization and Bandwidth Estimation of WSN for Data Centric Protocols", International Journal Of System Assurance Engineering And Management (2015).

[9] Rajkumar, Vani B. A, G. Rajaraman, Dr. H G ChandrakanthRajkumar et al."Security Attacks and its Countermeasures in Wireless Sensor Networks",Int. Journal of Engineering Research and Applications Vol. 4, Issue 10(Part -1), October (2014), pp.04-15.

[10] Zeng, R. "The Security Issues and Common Attacks in Wireless Sensor Networks", AMR, 998-999, 1299-1304(2014).

[11] Zeng, R.."Applied Technology for Typical Attacks and Security Mechanisms in Wireless Sensor Networks", AMR, 977, 484-490. (2014).

[12] Biswas, S. &Adhikari, S. "A Survey of Security Attacks, Defenses and Security Mechanisms in Wireless Sensor Network", International Journal Of Computer Applications, 131(17), 28-35. (2015).

[13] Anthony D. Wood and John A. Stankovic," A Taxonomy for Denial-of-Service Attacks in Wireless Sensor Networks", Department of Computer Science University of Virginia.

[14] Abdus Salam, M. &Halemani, N.."Performance Evaluation of Wireless Sensor Network Under Hello Flood Attack", IJCNC, 8(2), 77-87. (2016).

[15] Nayak, P., V.Bhavani, V., &B.Lavanya, B., "Impact of Black Hole and Sink Hole Attacks on Routing Protocols for WSN", International Journal Of Computer Applications, 116(4), 42-46. (2015).

[16] FirdousKausar, Eisa Al Eisa, Imam Bakhsh, "Intelligent Home Monitoring Using Rssi In Wireless Sensor Networks", International Journal Of Computer Networks & Communications (IJCNC) Vol.4, No.6, November (2012).

DOI 10.17148/IARJSET.2017.4401