Contemporary Engineering Sciences, Vol. 7, 2014, no. 3, 135 - 147
HIKARI Ltd, www.m-hikari.com
http://dx.doi.org/10.12988/ces.2014.3949

A Survey on Security Mechanisms and Attacks in Wireless Sensor Networks

Anser Ghazzaal Ali Alquraishee and Jayaprakash Kar

Department of Information Systems
Faculty of Computing & Information Technology
King Abdulaziz University, Kingdom of Saudi Arabia
jayaprakashkar@yahoo.com

Abstract

A Wireless Sensor Networks (WSNs) are applied in numerous important applications in target of tracking, military, remote environmental monitoring, health care application, ecological, and many others. Wireless Network Systems consists of a large number of tiny sensor nodes which are typically deployed in hostile environments where they are encountered a large variety of malicious attacks. The role of these tiny sensors nodes are these sense data and process. Finally formulate to organize Wireless Sensor Networks. WSNs have limited constraints, includes limited energy resources, low power, less storage space and memory, low computation capability, and short communication range. Due to these constraints a great challenge in security comes to the research community. This article briefs a survey on security mechanisms and attacks in WSNs.

Keywords: malicious attacks, energy resources, sensor security,unreliable communication

1 Introduction

A WSN is the collection of tiny sensor nodes having a base station. Functions of these nodes are they can efficiently to collect information and return to a base station. The hardware architecture of sensor node is it comprises of four fundamental units as sensing, processing unit, transceiver and a power unit along with some others components such as power generator, mobilzaor and location and area finding systems [3]. Hardware architecture of Sensing units is ti comprises two subunits: analog to digital converter and sensor unit. Function of converter is it converts the analog signal that is generated by the sensors to digital signals. Power unit such as single battery is used and is of compatible of power scavenging devices. The procedures that operate to collaborate the sensor nodes with other nodes are managed by processing units which connects to small storage unit. Transceiver unit is used to connect the nodes to the network. The mechanism use for network routing and the procedure use for sensing need information of position of nodes. This can be provided by a location finding system. Lastly, the mobilizer shifts the sensor node based on the application. The layers contains in the protocol stack are described below [3]:

- Physical layer: Selection of frequency, modulation, detection of signal, data encryption and carrier frequency generation are executed in this layer.

- Data link layer: detection of data frame, error control,access of medium and multiplexing of data streams are operated in this layer. Also this layer trust host-to-host and host-to-multi host connections.

- Network layer: This layer assigns address and responsible for routing of packets.

- Transport layer: The transports of reliable and trusted packets are done in this layer.

- Application layer: The data are requested by the sensor nodes and interact with the end users. The function that is used for this operation is done in this layer.

2 Organization of the article

The paper is organized as the first three section briefs the communication architecture, different Obstacles of Sensor Security and the most important security goals respectively. Section four and five describes the security mechanisms that is used as a countermeasure for the security attacks. Finally we brief the most important attacks in WSNs.

3 Constraints resources and Challenges

3.1 Limited Memory and Storage Space

Due to limited storage space and memory of the tiny sensor node, if we want to design an secure and efficient security protocols, it is required to develop the programs with less time and space complexity. For example, if we takes the sensor type TelosB which is having 48K program memory of 16-bit and 8 MHz. The storage capacity flash is 1024K [5] [14]. On this constraint memory and storage, the software develop for the sensor must have minimum complexity of time and space. For example The space complexity of TinyOS is 4K and the capacity of core scheduler is 178 bytes [4] [7].

3.2 Power Limitation Energy

Power energy is very limited in Sensor nodes. The operating cost and recharged are very high, when a node is replaced in a deployed network. On the implementation of cryptographic protocols, the energy required for additional security codes is to be considered The additional power energy inspired by sensor nodes is connected to the dispensation required for cryptographic operation such as ciphering and de-ciphering of message, generation and verification of signature. Also the additional power energy is required to transmit and store the security parameters of cryptographic keys [6].

4 Untrustworthy Communication

One of the most important threat unreliable communication media which is a vulnerability to sensor node. The impact of security of WSN depend on communication protocol in the following aspects [19]:

4.1 Conflicts

Due to broadcast nature, we can not assure the communication is reliable. In the middle of the sending and receiving of packets, conflicts may come which leads a failure transfer. This is a very serious problem in a high density sensor network [13].

4.2 Unreliable

In packet-based routing, transferring of packet in WSN is normally connectionless. Therefore it is intrinsically unreliable. Due to error in communication channel, Packets may get corrupted which consequence is packet's loss. Also the untrustworthy the communication channel in WSNs causes the corrupts of packets. Critical security packets are lost, if the protocol cannot perform the exact handing of error [12].

4.3 Latency

It is impossible to possess a proper synchronization among the sensor nodes due to network congestion, node processing and the multi-hop routing. This causes a greater latency. The proper synchronization among the nodes is vital to sensor security where the security primitives and protocols trust on significant cryptographic operations [11].

4.4 Exposure to Physical Attacks

Basically the tiny sensor mode are surrounded by malicious attackers and deployed in an environment of bad weather. The chances of physical attack on sensor nodes is more than the others secure network system. It is difficult to detect physical tempering through temper proof protection. Also it is impossible for physical maintenance like battery replacement [18].

4.5 No Central Management Point

There is no any central management point when the sensor nodes are clustered in distributed network.

5 Security Requirements

The most important security requirements in WSNs are confidentiality, integrity, availability, data freshness, secure localization, self organization and authentication. To establish a secure network system, we must have to achieve these security goals [1].

5.1 Data Confidentiality

One of the most important security requirements in WSNs is data confidentiality where the sensitive data are stored in the form of cipher text. The confidentiality is associated with [2]

- In many applications nodes transmit the secret parameters like distribution of key. Hence it is desired to construct a secure channel in a WSNs.

- To make resistant against traffic analysis attacks, the publicly known sensor information such as public keys, sensor node's identity, have to be encrypted.

5.2 Data Integrity

When transmitting the data through a secure channel, it cannot be assured that, the same information the receiver receives. The attacker might modify or alter the sensitive data which causes confusion in the sensor network. For example, some wreckage might be added in the packet by the malicious node which is sent to the original receiver. So the integrity in data may not be preserved. Also because of insensitive communication environment, possibilities are there in Data loss or damage, even though there does not exist malicious node [18].

5.3 Data Freshness

For a secure wireless sensor network, also we should achieve data freshness of each message along with confidentiality and integrity [14]. Data freshness of a message suggests that the data is current, and it ensures that no previous messages have been replayed. This requirement is very essential in key establishment protocols. It is important to change the session key over time.

5.4 Availability

Implementing the conventional cryptosystem to robust within the WSNs take additional computational costs. Some technique needs to alter the code to reuse as much as possible. Certain techniques are there that use extra communication to achieve the same goal. Also some technique might severe confines on the data access, or proposes an inappropriate mechanism for simplification of the algorithm. Due to the following, the technique deteriorate the availability of a sensor and sensor network [18]:

- There consume additional energy for additional computation. The data will no more alive, if it does not get energy.

- Additional communication increases the bandwidth and consumes huge energy.

- Application of central point mechanism causes failure in single point. This is vulnerability of the availability of the Sensor Network. It is very to maintain the availability of the network.

5.5 Self-Organization

In WSNs, each and every sensor node need to be independent and supple more to be self-organizing to various positions. The communications among the nodes and base station are not fixed [8]. This essential feature leads a massive challenge to the security of WSNs.

5.6 Secure Localization

Function of a sensor network trust on its capability to locate each sensor in the network automatically and properly. A sensor network is designed to locate information to identify the error's position But, an unintended user can manipulate easily the unsecured position of information by exposing replying signals. The location of device is correctly calculated from a series of known reference points. This technique is known as verifiable multi-alteration [24] .

5.7 Authentication

An adversary can not only alter the packet but can modify the entire data stream of packet by appending some false packets. Therefore it is needed for the receiver needs that the data used in any precise work, came from the right sender. Hence authentication is required for controlling cycle of sensor node and network programming. Therefore authentication provides a receiver to verify that the data exactly is sent by the claimed sender.

6 Security Mechanisms and Protocols

This section describes the security mechanism and protocols that are use as countermeasure of the security attack. Security mechanisms is applied to detect recuperate and thwart from attacks. The security mechanism is classified as low and high level. The most important low-level security protocols/primitives are

- Key agreement Protocol
- Authentication Protocol
- Resilience to node capture
- Privacy or Confidentiality
- Robustness to communication
- Secure routing

6.1 Key Agreement Protocol

Due to limitation of energy and computational power, public key cryptographic protocols are too costly to implement. Communication topology of sensor networks be at variance from conventional networks. It is required to establish key for sensor nodes with the neighboring and data aggregation nodes. The vulnerability of this technique is that attackers use large number of nodes could also reconstruct the complete key and crack the technique.[1] Due to resources constraints, public key cryptosystem is not suitable for implementation. So the scheme based on Symmetric key cryptography are suitable for sensor networks. However, a most important insufficiency of symmetric cryptography is key management problem. It is difficult to establish a provably secure keys among neighboring nodes in a WSN.

6.2 Authentication Protocol

It is required to protect against unintended users, eavesdropping and altering or modification of packets in sensor network applications. For host -to-host communication [12] , cryptographic primitives achieves a high level of security but it is needed to establish the keys among all end points and be unsuited with local broadcast and inactive involvement. A link-layer cryptographic primitive in sensor network simplifies the set up of cryptographic key.

6.3 Secure routing

Data forwarding and Routing are vital countermeasure to establish communication in WSNs. There are vulnerabilities in existing routing protocols. Suppose an attacker applies denial of-service attacks on the routing protocol. By injecting malicious routing information into the sensor network, The simplest attacks absorb and result in routing inconsistency.

6.4 Resilience to node capture

In many applications, sensor nodes are probable to be arranged locations easily accessible to attackers. Such revelation raises the opportunity to the adversary that, he may capture nodes, take out secret parameters used in the cryptographic protocols, alter the program, or replace them with malicious nodes under the control of the adversary. The countermeasure use is Tamper-resistant wrapping, but it’s expensive since need costly operation. It is noot possible to provide a high level of security in the current technique. The countermeasure for node capture is required a Secure and efficient Cryptographic protocols/primitive is the countermeasure to the node capture problem. [1]

To secure sensor network, high-level security mechanisms are required. These are secure group management, securing sensor networks, securing data aggregation, and intrusion detection.

6.5 Secure group management

Even though the Computational and communication power of each sensor node is limited, data aggregation, cryptographic computation and analysis are done by a cluster of nodes. A cluster of nodes might be responsible for jointly tracking a vehicle through the network The power of communicating and computing are constraints for every sensor node. Analysis and data aggregation are performed by groups of nodes.

6.6 Intrusion detection

WSNs are vulnerable to several forms of intrusion. The solution for decentralize intrusion detection is to use a secure groups, that must be fully distributed and of low communicational cost, low memory and energy [15].

6.7 Secure data aggregation

To remove irresistible amounts of traffic back to the base station, it is required to aggregate the sensed values. In many places of sensor network depending on the deployment of sensor nodes , aggregation is essential Depending on the topology of the wireless sensor network, aggregation is required in many places in the network [22].

7 Attacks on WSNs

Wireless Network Systems composed of a large number of sensor nodes which are typically deployed in hostile environments where they are encountered a large variety of malicious attacks. Sensor networks are vulnerability to a diversity of attacks on the different layers. The most important attack is denial of service attacks. Apart from this attack other attacks are privacy violation, traffic attack, Monitoring and eavesdropping, physical attacks, node capture and so on [21]. The most important challenging attacks on WSNs are Physical Layer DoS, Link Layer DoS, Attacks on Transport Layer, Attacks on Routing, Sybil attack and Attacks on Data Aggregation

8 Denial-of-Service

In this type of attack, attacker disconnects the network from operation or interrupt the function of network. DoS attacks can take place at different layers of the protocol stack. Because of probable irregularity in computational and power limitation protecting against harm, DoS attack on a WSNs is impossible [9]. Sensor node might be jammed by more powerful node and efficiently protect the sensor network from executing its anticipated operation.

8.1 Physical Layer DoS

When the attacker interfaces with radio frequencies of WSNs, the jamming attack take place. If efficiently and well organized, a small number node that are attacking can immobilize an whole network, yet the number of nodes in the network is more greater than the number of attacking nodes. If the attacking node is positioned near to the gateway, then the node can immobilize the entire network. Therefore to protect the data in the sensor node from send-off the sensor network or the power of transmission is large such that all nodes may be protected from properly receiving significant data. A well known method against jamming is applied to spread-spectrum communication, as specified in IEEE 802.11 and Blue tooth. Based on a particular hopping sequence, communicating devices, frequency-hopping spread spectrum, frequently fluctuates between frequencies. For continuous interruption, this sequence should either be known by a jammer or be jammed by frequency band to capable to jam the exact frequency. The Sensor network's control can detect and take action to these attacks in sensor network. In order to conserve energy by changing nodes into sleep modes of low power, while developing them from time to time to verify if it is active or not. To information the vulnerability of attack, nodes alert a base station or gateway. In the direction of this end, nodes detecting a jamming attack communicate a summary of alerts to their neighboring nodes [17]. The message can be broadcast to the other nodes and the base station, even if one of these neighboring nodes lays in exterior the area of the attack. When an adversary is allowed for physical access to a sensor node, tampering attack occurs which destroys or modifies the device. This leads to capture the secret information like private keys information and use the device for future attack. The countermeasure to protect from tampering is to use tamper-proof materials and removed the information, when the attack is detected.

8.2 Link Layer DoS

Link layer DoS is the collision attack. This attempt to obstruct with packet transmissions and causes expensive exponential back off procedures and retransmission in message authentication protocol (MAC). It is not possible to recover from corrupted bits having all types of interfaces in a packet by using error-correcting code [20]. Therefore it acquires additional resources and energy. An attacker might endeavor to form collisions near the end of a frame. The goal of an attacker might be to generate the impulsive exhaustion of the energy resources of node.This is known as exhaustion attack.

8.3 Attacks on Routing

In this type of attack, attacker create routing loop and attract or repel network traffic, create fake routing messages, and mortify the network performance by spoofing, modifying or replaying routing information Black hole attack is a type of attack on routing protocols in WSNs. Here, attacker forward the sensitive data multiple routes across the network. Another type of similar attack is selective forwarding attack, instead of dropping all packets arbitrarily , dropped only packets that satisfy particular condition . These type of attacks are infeasible to detect the black hole attacks since they are difficult to differentiate from losses of packet. The vulnerability of route discovery technique of on demand routing protocols is exploited by rushing attack. Here, a malicious node straight away forwards inward route call messages to its neighboring nodes, hence ”rushing” these messages lacking contemplation of any protocol rules. As a result, the sensor node has maximum chances of being element of the selected route between source and destination [19]. Another type of black hole attack is Sinkhole attack. In this type of attack, the malicious node attempts to place itself on the rout of various network flows. Therefore traffic is strained toward the sinkhole which provides the facilities to the adversary to interrupt or temper [1].

Another type of attack is Sybil attack. In this type of attack the adversary shows multiple identities in the sensor network. In routing protocols that are based on location, the attacker demand to have multiple location concurrently [5]. Wormhole attack is an attack on routing protocol. The sensor nodes which have more resources, performs this attack. Two collaborating attackers process band width rich communication channel between them and attempt to mislead the respite of the sensor network [23]. Using this technique, attacker node counterfeit the short path to the gateway of a network.

8.4 Attacks on Transport Layer

End-to end connection is managed by transport layer. The two most important protocols for transport layer are User Datagram Protocol and Transmission Control Protocol for trusted stream-based communication and unreliable packet-based communication respectively. When an attacker requests new connection frequently, that includes more state information at the exaggerated node and potentially leads to node refusing again connections because of resource exhaustion [16]. This in revolve prevents connection requests legitimate nodes from the subsequent. De-synchronization attack is the attack in which, an attacker attempts to interrupt the communication between two valid nodes by forging messages to these nodes frequently. In order to monitor the received packets, detect duplication and loss of packets are identified.An adversary issues fake packet and use these sequence number to enable a node to rely That the packets reached at the destination

9 Conclusion

Sensor nodes which are typically deployed in hostile environments where they are encountered a large variety of malicious attacks. Sensor networks are vulnerability to a diversity of attacks on the different layers. Here we have described the most important attacks on WSNS and the security mechanism that are used as countermeasure. Also we describes the attack other attacks includes privacy violation, traffic attack, Monitoring and eavesdropping, physical attacks, node capture.

References

[1] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci. A survey on sensor networks, IEEE Communications Magazine 40(8):102114, August 2002.

[2] P. Albers and O. Camp. Security in ad hoc networks: A general intrusion detection architecture enhancing trust based approaches,4^{th} International Conference on Enterprise Information Systems, 2002.

[3] Perrig A., Stankovic J., Wagner D. Security in Wireless Sensor Networks, Communications of the ACM, 47(6), 53-57, 2004.

[4] R. Anderson and M. Kuhn. Tamper resistance - a cautionary note. In The Second USENIX Workshop on Electronic Commerce Proceedings, Oakland, California, 1996.

[5] T. Aura, P. Nikander, and J. Leiwo. Dos-resistant authentication with client puzzles. In Revised Papers from the 8th International Workshop on Security Protocols, pages 170177. Springer-Verlag, 2001.

[6] A. R. Beresford and F. Stajano. Location Privacy in Pervasive Computing. IEEE Pervasive Computing, 2(1):4655, 2003.

[7] R. Anderson and M. Kuhn. Low cost attacks on tamper resistant devices. In IWSP: International Workshop on Security Protocols, LNCS, 1997.

[8] P. Bose, P. Morin, I. Stojmenovic;, and J. Urrutia Routing with guaranteed delivery in ad hoc wireless networks & Wireless Sensor Network., 7(6):609616, 2001.

[9] Bryan Parno, Adrian Perrig, Virgil Gligor. Distributed Detection of Node Replication Attacks in Sensor Networks, pp. 49-63, 2005 IEEE Symposium on Security and Privacy (S&P'05), 2005

[10] L. Hu and D. Evans Using directional antennas to prevent wormhole attacks. In 11th Annual Network and Distributed System Security Symposium,February 2004.

[11] D. Braginsky and D. Estrin. Rumor routing algorthim for sensor networks. In WSNA 02: Proceedings of the 1st ACM international workshop on Wireless Sensor Network and applications, pages 2231, New York, NY, USA, 2002,ACM Press.

[12] J. Deng, R. Han, and S. Mishra. Security, privacy, and fault tolerance in wireless sensor networks. Artech House, August 2005.

[13] J. Newsome et al. The Sybil Attack in Sensor Networks: Analysis and Defenses, IPSN '04: Proc. IEEE Int'l. Conf. Info. Processing in Sensor Networks, Apr. 2004.

[14] C. Hartung, J. Balasalle, and R. Han. Node compromise in sensor networks:The need for secure systems. Technical Report Technical Report CU-CS-988-04, Department of Computer Science, University of Colorado at Boulder, 2004.

[15] L. Hu and D. Evans. Secure aggregation for wireless networks. In SAINTW 03: Proceedings of the 2003 Symposium on Applications and the Internet Workshops, page 384. IEEE Computer Society, 2003.

[16] Y. Hu, A. Perrig, and D. B. Johnson Packet leashes: a defense against wormhole attacks in wireless networks. In INFOCOM 2003. Twenty-Second Annual Joint Conference of the IEEE Computer and Communications Societies., volume 3, pages 19761986, 2003.

[17] Q. Huang, J. Cukier, H. Kobayashi, B. Liu, and J. Zhang Fast authenticated key establishment protocols for self-organizing sensor networks. In Proceedings of the 2nd ACM international conference on Wireless sensor networks and applications, pages 141150. ACM Press, 2003.

[18] J. Hwang and Y. Kim. Revisiting random key pre-distribution schemes for wireless sensor networks. In Proceedings of the 2nd ACM workshop on Security of Ad hoc and Sensor Networks (SASN 04), pages 4352, New York, NY, USA, 2004. ACM Press.

[19] H. Chan and A. Perrig. Security and Privacy in Sensor Network IEEE Communications Surveys & Tutorials 2nd Quarter 2006 works, IEEE Comp. Mag., Oct. 2003, pp. 10305.

[20] F. Ye et al. Statistical En-Route Filtering of Injected False Data sensor Networks, IEEE Proceeding of IFOCOM, Hong Kong, 2004.

[21] W. Du et al. A Pairwise Key Predistribution Scheme for Wireless Sensor Networks, CCS 03: Proc. 10th ACM Conference Computer and Communications Security, New York: ACM Press, 2003, pp. 4251.

[22] J. Girao, D. Westhoff, and M. Schneider CDA: Concealed Data Aggregation for Reverse Multicast Traffic wireless Sensor Networks, ICC 05: Proceeding of IEEE International conference of Communication, Seoul, Korea, May 2005.

[23] J. N. Al-Karaki and A. E. Kamal Routing Techniques in Wireless Sensor Networks: A Survey, IEEE Wireless Communication 11(6), Dec. 2004, pp. 628.

[24] Jeong, J., Jiang, X. F. and Culler, D. E. Design and Analysis of Micro-Solar Power Systems for Wireless Sensor Networks, Electrical Engineering and Computer Sciences, University of California at Berkeley, 2007,Technical Report PMM03 R. D. Pietro, L. V. Mancini, and A. Mei Random Key-Assignment for Secure Wireless Sensor Networks, SASN 03: Proceeding. 1st ACM Wksp. Security of Ad Hoc and Sensor Networks, New York: ACM Press, pp. 6271,2003.

[25] J. Lee and D. R. Stinson A Combinatorial Approach to Key Predistribution for Distributed Sensor Networks, Proceeding of IEEE Wireless Communication and Networking 2005.

Received: September 1, 2013