International Journal of Mathematical Archive-10(5), 2019, 45-48
Available online through www.ijma.info ISSN 2229 – 5046

A REVIEW ON WIRELESS SENSOR NETWORK SECURITY THREATS

HIMANSHU SIROHI
Department of Computer Applications,
Swami Vivekanand Subharti University, Meerut - (U.P.), India.

SUNIL KUMAR*
Department of Mathematics,
Swami Vivekanand Subharti University, Meerut - (U.P.), India.

(Received On: 06-03-19; Revised & Accepted On: 02-05-19)

ABSTRACT

Wireless sensor network (WSN) is denotes to a group of isolated and enthusiastic sensors for observing and footage the physical conditions of the environment and establishing the collected data at a central place. Wireless sensor network is a mixture of small devices called as sensor nodes which have calculating, sensing and treating capabilities. Different application areas of WSN's are Environmental Checking, Industrial Identifying, Organization Security, Fight Field Awareness, Situation Alert Computing etc. The attachment of wireless communication knowledge also experiences several types of security threats. Information in the network must be secure from the invaders. Various types of security threats have been identified for Sensor Net Setting. Future possibility of the work has also been outlined.

Key Words: *Wireless Sensor Networks, Security, Threats, Attack, Secure Information.*

I. INTRODUCTION

Wireless sensor network (WSN) may be classified as a network of devices those can interconnect the facts collected from an observed field over wireless links. The data is sent over multiple nodes, and with a gateway. A Wireless Sensor Networks have grown much popularity and consideration since the last few years. The main reason for WSN acceptance is that it can work in critical applications like battle filed application, weather forecasting, health observing etc. Collecting the information from the physical world is one of the primary goals for wireless sensor networks. Wireless sensor network (WSN) is structure independent, where they can be constructed effectively to work in any harsh environment, without the need of wired connection.

In wireless sensor network each node contains some components like a controller, transceiver, outer memory, power source. One other component is base stations, which performed as a gateway among the sensor nodes and end user. To make Wireless sensor network possible for all kinds of applications at lower cost we need simple protocols for communication, security, topology management, medium access control which are supposed to be energy efficient. Though security is a very important issue in WSN, very little work is available for securing a WSN.

To understand the boundaries of present security mechanisms it is essential to understand the features of a wireless sensor network. Different features of WSN such as low energy, low memory, low bandwidth for communication and large scale nodes make most of the present security solutions available for other ad-hoc and wired networks impractical for WSNs. We have identified different challenges in providing security to a WSN deployment. These are given below.

Fault-Tolerance: In an antagonistic environment, a sensor node may flop due to physical loss or lack of energy. If some nodes flop, the protocols that are working on must accommodate these alterations in the network.

Scalability: Many applications are needed; the large number of sensor nodes arranged must be in an order of hundreds or more. The protocols must accessible enough to respond and operate with such large number of sensor nodes.

Corresponding Author: Sunil Kumar*
Department of Mathematics, Swami Vivekanand Subharti University, Meerut-(U.P.), India.

Physical Resource Constraints: The most imperative constraint compulsory on sensor network is the limited battery power of sensor nodes. The lifetime of a sensor node is directly calculated by its power supply. Hence the energy consumption is main design problem of a protocol. The another limitation is Limited computational power and memory size that influence in the amount of data that can be stored in separate sensor nodes. So, the protocol should be light-weighted and simple. Communication delay in sensor network can be high due to limited communication channel shared by all nodes within each other's transmission range.

Ad-hoc Deployment: Many applications are requires the ad-hoc deployment of sensor nodes in the special area. Sensor nodes are casually arranged over the region without any organization and earlier knowledge of topology. In this condition, it is depends on the nodes to recognize its connectivity and distribution between the nodes.

Quality of Service: Some real time sensor application are very time critical which means the data should be distributed within a certain period of time from the moment ,it is sensed and checked, otherwise the data will be unusable .So this must be a QOS(Quality of services) parameter for some applications.

Security: Security is very critical parameter in sensor networks, given some of the proposed applications. An effective compromise must be obtained, between the low bandwidth requirements of sensor network applications and security demands for secure data communication in the sensor networks.

II. SAFETY AND SECURITY REQUIREMENTS IN WIRELES SENSOR NETWORKS

The spatially distributed self-ruling sensors are contains by WSN (the wireless sensor network) for monitoring the condition of environment. Wireless sensor network development is based on military applications. In military WSN is used in battle-line surveillance. Wireless Sensor Networks (WSN) worked at very difficult places like surveillance, observing, airports, battle-line applications. Hence for providing security in wireless sensor networks is a very difficult task. Following are the Security Requirements in Wireless Sensor Networks.

1. Confidentiality: Confidentiality requirement is required to certify that delicate information is well secured and not exposed to unauthorized third parties .The main purpose of confidentiality requirement that the information move among the sensor nodes of the network or between the sensors, since an adversary having the appropriate equipment may eavesdrop on the communication. By eavesdropping, the adversary could overhear critical information such as sensing data and routing information. Based on the sensitivity of the data stolen, an adversary may cause severe damage since he can use the sensing data for many illegal purposes i.e. sabotage blackmail. For example, safety monitoring sensor application. Furthermore, by stealing routing information the adversary could introduce his own malicious nodes into the network in an attempt to overhear the entire communication.

2. Authentication: Data authentication agrees a receiver to validate that the data really is sent by the requested sender. In the event of two-party communication, data authentication can be completed by a purely symmetric tool (mechanism). The both sender and the receiver shared a secret key to calculate the MAC (Message authentication code) for all communicated data.

3. Integrity: The objective of integrity, there is a situation that information could be transformed when switched over insecure networks. Deficiency of integrity creates many problems since the significances of using inaccurate information could be disastrous. Integrity controls must be applied to ensure that information will not be altered in any unexpected way.

4. Time Synchronization: A sensor may wish to evaluate the end-to end interval of a packet. It moves among two pair wise sensors. A more combined sensor network may require group synchronization for tracking the applications, etc.

5. Secure Localization: A sensor network will trust on its ability to correctly and automatically find each sensor in the network. A sensor network intended to find faults will need correct location information in order to pinpoint the location of a fault.

6. Secure Management: Management is needed in every system that is established by multiple components and handles delicate information. In the case of sensor networks, we need protected management.

III. THREATS AND DIFFERENT LAYERS IN WIRELESS SENSOR NETWORKS

A. **Physical layer**: Communication media is wireless is open, so high security risk is there. Some of those security threats are:

- **JAMMING**: Jamming is a general Denial of service (DOS) attack on physical layer of network. In jamming, adversaries interferes with the communication frequencies (radio frequencies) being used by the nodes of the network. In jamming, an attacker can concurrently transmit over the WSN refusing the underlying MAC Protocol. Jamming can affect the whole network if single frequency is used throughout the network.

- **TAMPERING**: One another attack in physical layer is tempering. In this type of attack, an adversary may compromise some of the legitimate sensor nodes in the network and using these nodes, he/she may carry out lots of misleading activities in the network.
- **SYBIL ATTACK**: An adversary node assumes uniqueness of multiple nodes. This may causes ineffectiveness in wireless sensor network.

B. Data link layer: Attacks can also be possible in data link layer. Some of those security threats are:

- **COLLISION:** In this type of DOS attack, an adversary may induce small change in data portion of the packet and which may lead to error in checksum calculation and may cause retransmission of data packets.
- **EXHAUSTION:** In exhaustion attack, an adversary may uninterruptedly disturb the communication among two nodes and affect the sensor node to retransmit again and again. This may lead to quick energy decay.
- **TRAFFIC ANALYSIS:** Communication design of a sensor network can be examined by an adversary. That will cause harmful effect on the network.
- **SYBIL ATTACK:** In this layer Sybil attack is very much effective. There are two different variations in Sybil attack.
  - **Data aggregation**- A single mischievous node may work as different Sybil nodes and these nodes may provide many negative reinforcements for making the aggregate message to a false one.
  - **Voting**: An attacker may be accomplished to define the outcome of any voting depending on the no. of identities the attacker owns.

C. Network layer: Major security goal of network layers are:

- Every intended receiver node should receive all messages and the intended receiver also verifies the ID of source of node and integrity of message.
- Routing protocol should be responsible for controlling the eavesdropping. WSN network layer are vulnerable to various attacks. Broadly, they are categorized in two types:
  - **Passive attack-** An adversary can only discover information without modifying them. It is tough to find out these attacks.
  - **Active attack-** An adversary can change the information and thus interfere in various operation of the network. An attacker can change both routing as well as data packets causing false routing table at source and imperfect communication. E.g. - Wormhole attack.

D. Transport Layer: The responsibility of transport layer is for managing end-to-end connections .Attacks on these layers is:

- **Flooding**: When a protocol is needed to maintain state at either end of a connection. So it becomes susceptible to memory exhaustion through flooding. An attacker may repetitively make new connection requests until the resources required by each connection are exhausted or reach a maximum limit. In either case, further legitimate requests will be ignored. One proposed solution to this problem is to require that each connecting client demonstrate its commitment to the connection by solving a puzzle. The idea is that a connecting client will not needlessly waste its resources creating unnecessary connection. Given that an attacker does not likely have infinite resources, it will be impossible for him/her to create new connections fast enough to cause resource starvation on the serving node. While these puzzles do include processing overhead, this technique is more desirable than excessive communication.
- **De-synchronization:** it may be classified as the disruption of an existing connection. An attacker can repetitively spoof messages to an end host, causing that host to request the retransmission of missed frames. If timed appropriately, an attacker may degrade the ability of the end hosts to successfully interchange data, thus causing them to instead waste energy by attempting to recover from errors which never really existed. A possible solution to this type of attack is to require authentication of all packets communicated between host's .Provided that the authentication method is itself secure; an attacker will be unable to send the spoofed messages to the end hosts.

IV. CONCLUSION

Security issue in wireless Sensor Network is more important than other issue. In recent years, security in WSN has frequently concerns. Wireless sensor networks are growing used in environment, commercial, health and military applications. This paper briefs a sort of requirements that wireless sensor network have to be include and also introduce some of the security attacks.

REFERENCES

1. Xiuli Ren and Haibin Yu1." Security mechanisms for wireless sensor networks". IJCSNS International Journal of Computer Science and Network Security, VOL.6(No.3):100-107, March 2006.
2. P.Nair H.Cam, S.Ozdemir and D. Muthuavinashiappan. Espda. "Energy-efficient and secure pattern based data aggregation for wireless sensor networks". Computer Communications IEEE Sensors, 29:446-455, 2006.
3. Corke, P., Sen, S., Sikka, P., Valencia, P. and Wark, T. (2006)" Wireless sensor and actuator networks". CSIRO, 2-year Progress Report: July 2004 – June 2006.
4. A. S. Wander, N. Gura, H. Eberle, V. Gupta, and S. C. Shantz, "Energy analysis of publickey cryptography for wireless sensor networks," in Third IEEE International Conference on Pervasive Coinputing and Communications (PERCOM'05). IEEE Computer Society Press, 2005, pp. 324-328.
5. Ismail H. Kasimoglui Ian .F. Akyildiz. "Wireless sensor and actor :research challenges". (Elsevier) Journal, 2(38):351367, 2004.
6. E. Shi and A. Perrig, "Designing Secure Sensor Networks," Wireless Commun. Mag., vol. 11, no. 6, Dec. 2004 pp. 38–43.
7. H. Yang, H. Luo, F. Ye, S. Lu, and L. Zhang, "Security in mobile ad hoc networks: challenges and solutions," IEEE Wireless Communications, vol. 11, no. 1, pp. 38-47, Feb. 2004.
8. A. Perrig, J. Stankovic, and D. Wagner, "Security in wireless sensor networks," Commun. ACM, vol. 47, no. 6, pp. 53-57, 2004.
9. C. Karlof and D. Wagner, "Secure Routing in Sensor Networks: Attacks and Countermeasures," Proc. 1st IEEE Int'l. Wksp. Sensor Network Protocols and Apps., 2003.
10. Kumar.S.P. Chee-Yee Chong. "Sensor networks: Evolution, opportunities, and Challenges". Proc IEEE, August 2003.
11. H. Chan and A. Perrig, "Security and Privacy in Sensor Net works," IEEE Comp. Mag., Oct. 2003, pp. 103–05.
12. A. D. Wood and J. A. Stankovic, "Denial of Service in Sensor Networks," Computer, vol. 35, no. 10, Oct. 2002, pp. 54–62.
13. I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci." A survey on sensor networks". IEEE Communications Magazine 40(8):102–114, Aug. 2002.
14. D. Estrin et al., "Instrumenting the World with Wireless Sensor Networks," Proc. Int'l. Conf. Acoustics, Speech and Signal Processing, Salt Lake City, UT, May 2001.
15. D. Carman, B. Matt, D. Balenson, and P. Kruus, "A communications security architecture and cryptographic mechanisms for distributed sensor networks," in DARPA SensIT Workshop. NAI Labs, The Security Research Division Network Associates, Inc., 1999.

Source of support: Nil, Conflict of interest: None Declared.