AJCSE
ASIAN JOURNAL OF COMPUTER SCIENCE ENGINEERING

www.ajcse.info

Asian Journal of Computer Science Engineering 2016; 1(2):29-34

REVIEW ARTICLE

Wireless Sensor Networks: An Overview on Security Issues and Challenges

***Arundhati Nelli[1], Sushant Mangasuli[2]**

[1,2]Visvesvaraya Technological University BELGAUM

Received on: 20/10/2016, Revised on: 14/11/2016, Accepted on: 01/12/2016

ABSTRACT

Wireless Sensor Networks (WSNs) are formed by deploying as large number of sensor nodes in an area for the surveillance of generally remote locations. A typical sensor node is made up of different components to perform the task of sensing, processing and transmitting data. WSNs are used for many applications in diverse forms from indoor deployment to outdoor deployment. The basic requirement of every application is to use the secured network. Providing security to the sensor network is a very challenging issue along with saving its energy. Many security threats may affect the functioning of these networks. WSNs must be secured to keep an attacker from hindering the delivery of sensor information and from forging sensor information as these networks are build for remote surveillance and unauthorized changes in the sensed data may lead to wrong information to the decision makers. This paper gives brief description about various security issues and security threats in WSNs.

Keywords: Sensor, Security, Threats, wireless, overview, Challenges.

INTRODUCTION

Wireless Sensor Networks (WSN) are emerging as both an important new tier in the IT ecosystem and a rich domain of active research involving hardware and system design, networking, distributed algorithms, programming models, data management, security and social factors . The basic idea of sensor network is to disperse tiny sensing devices; which are capable of sensing some changes of incidents/parameters and communicating with other devices, over a specific geographic area for some specific purposes like target tracking, surveillance, environmental monitoring etc. Wireless Sensor Networks (WSNs) are the collectors of information from the physical world in the form of sensed data according to the requirement like temperature, pressure, humidity, level, movement etc. This data is available to the sink through gateway. Sensors are deployed in extensive numbers and on account of its wireless nature; it is easily works in any type of environment. Although sensor nodes are deployed in a random manner still it's important to deploy them carefully. Deploying few nodes may raise the issue of coverage and deploying too many nodes may result in an inefficient network because of more collision and interference. Wireless Sensor Networks (WSNs) need effective security mechanisms because these networks deployed in hostel unattended environments. Due to inherent limitations in wireless sensor networks, security is a crucial issue. While research in WSN security is progressing at tremendous pace, no comprehensive document lists the security issues and the threat models which pose unique threats to the wireless sensor networks.

We identify the security threats, review proposed security mechanisms for wireless sensor networks. Security in the Wireless Sensor Networks has various difficulties, some common are: dynamically changing topology, wireless communication among the sensor nodes, infrastructure-less framework, and limited physical resources like energy source, memory capacity and very low communication bandwidth . Numerous analysts proposed so many threats handling models and diverse security protocols for secure data communication and routing in WSN.

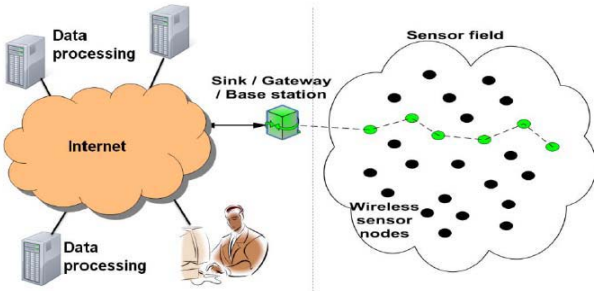

Fig 1: Architecture for WSN

***Corresponding Author:** Arundhati Nelli**, Email**: arundhati.nelli007@gmail.com

There are many parameters affect selecting the security mechanism as its speed and energy consumption. The intent of this paper is to investigate the security related issues and challenges in wireless sensor networks.

WSN SECURITY REQUIREMENTS

A WSN is a sensor node has the limited processing capacity, a limited storage capacity and limited communication bandwidth, limited energy and hardware size. There are so many types of the sensor nodes currently available on different platforms. The security also matter with the design of the hardware of sensor nodes in the real life. Sensor network have to fulfill some requirements for providing a secure communication. General security requirements of WSNs are availability, confidentiality, integrity and authentication. Some other requirements known as secondary requirements are source localization, self organization and data freshness. These requirements gives protection against attacks to the information transmitted over the sensor network.

Data Confidentiality: In sensor network, data flows from many intermediate nodes and chance of data leak is more. To provide the data confidentiality, an encrypted data is used so that only recipient decrypts the data to its original form.

Data Integrity: Data received by the receiver should not be altered or modified is Data Integrity. Original data is changed by intruder or due to harsh environment. The intruder may change the data according to its need and sends this new data to the receiver.

Data Authentication: It is the procedure of confirmation that the communicating node is the one that it claims to be. It is important for receiver node to do verification that the data is received from an authenticate node.

Data Availability: Data Availability means that the services are available all the time even in case of some attacks such as Denial of service.

Source Localization: For data transmission some applications use location information of the sink node. It is important to give security to the location information. Non-secured data can be controlled by the malicious node by sending false signal strengths or replaying signals.

Self-Organization: In WSN no fixed infrastructure exists, hence, every node is independent having properties of adaptation to the different situations and maintains self organizing and self healing properties. This is a great challenge for security in WSN.

Data Freshness: Data freshness means that each message transmitted over the channel is new and fresh. It guarantees that the old messages cannot be replayed by any node. This can be solved by adding some time related counter to check the freshness of the data.

Scalability: It should sustain a big number of nodes.

Time Synchronization: It should avoid collision and traffic manipulation.

OBSTACLES AND CONSTRAINTS

WSN is a wireless network which has several constraints as compared to other similar networks. These obstacles and restrictions make it complex to implement security techniques in WSNs. Therefore, to develop efficient security mechanisms it is necessary to know and comprehend and these obstacles, which are as follows:

Limited Resources: The scarcity of resources makes implementation of security techniques difficult as they need a certain amount of resources for operations e.g. data memory and processing power.

Unreliable Communication: The security of the network greatly depends upon the defined protocols and communication medium which is wireless in nature.

Unattended Operation: The sensor nodes may be left unattended for long periods of time as per the type of application of the particular WSN which make them more vulnerable to many attacks.

Due to these obstacles, the nodes and the network experience many constraints which further effect their overall functioning. For nodes the constraints are limited energy, memory, storage space and processing power. On the other hand due to these obstacles the network becomes untrusted and unreliable, collision prone and managed remotely with no or less resiliency.

CATEGORIES OF ATTACKS IN WSNs

The attacks those are effective in WSNs can be categorized by interruption and communication act in three categories:

1. **Outsider Vs Insider attacks:** In this WSN, outsider attacks may be known as external attacks and the insider attacks known as the internal attacks. An outsider attacks come from outside the WSN. With the help of Outsider attack the garbage data is injected in network for the services

interruption if network and a DoS attack is also rise. An insider attack is also known as the internal attack, these attacks come from the inside of the WSN, those attacks want to interrupt the running process in network and also exploit the network assets.

2. **Passive Vs Active Attacks:** Passive attack is easier to realize and not difficult to detect because it does not modify any information during the interchanged information. After analyzing the routing information we can make a active attack.In active attacks, an attacker has the capability to remove or modify the messages during the transmission on the network.
3. **Mote-class Vs laptop-class attacks** : In bit class assaults, an enemy assaults a WSN by utilizing a couple of hubs with comparative capacities to the system hubs; in portable PC class assaults, a foe can utilize all the more capable gadgets to assault a WSN. These gadgets have more noteworthy transmission reach, handling force, and vitality saves than the system hubs. In bit class assaults, an enemy assaults a WSN by utilizing a couple of hubs with comparable capacities as that of system hubs. In portable workstation class assaults, an enemy can utilize all the more capable gadgets like tablets, thus on and can do substantially more mischief to a system than a malicious sensor hub.

ATTACKS IN WSNs AT DIFFERENT LAYERS

1. **PHYSICAL LAYER**: "The first layer is physical layer that is responsible for frequency selection, carrier frequency generation, signal detection, modulation, and data encryption. As with any radio-based medium, there exists the possibility of jamming and interferences".
2. **Data Link Layer**: The next layer is data link layer that is in charge for the multiplexing of data streams, data frame detection, medium access, and error control, and responsible for point to point & point –to-multipoint relation in the network.
3. **Network and Routing Layer:** The third layer is network and routing layer provide more effective routing the data from "Node to node, node to sink, node to base station and node to Cluster head & vice versa." Due to the broadcast method every node works as a router.
4. **Transport Layer: "**The transport layer is responsible for managing end-to-end connections. In sensor network connection this layer is responsible to the communication. There are three possible attacks in this layer, flooding, resynchronization and false message injected.

The attacks on different layers and their defense are given in below table.

Layers	Attack types	Defense
Transport Layer	Flooding Desynchronization False message injected	Client puzzles, Rate limitation authentication
Network and Routing Layer	Black holes Sinkholes Sybil Information & selective forwarding Wormhole	Authentication, Monitoring, Redundancy verification, packet leashes by using geographic and temporal information. Redundancy Authorization, monitoring Egress Filtering and authentication
Data Link Layer	Jamming & Collision, Exhaustion, Unfairness	Error correcting Rate-limit Small frames
Physical Layer	Jamming Tempering	Speed Spectrum, Priority Messages Temper –proofing, hiding

SECURITY LEVELS

In this paper our overview report has concentrated on different

parts of sending secure conventions by the late analysts. Numerous specialists have proposed a wide range of systems to give security in imprompt remote systems. The use of these strategies to sensor systems is promising, however the likelihood of pernicious hubs coercing great hubs and the trouble in recognizing hub misconduct. All are valuable building pieces for securing directing conventions in sensor systems. To accomplish proficient key administration, a few symmetric key based systems were proposed previously. So that the study on symmetric key cryptography, as of late, there are various studies researching the execution of PKC (Public Key

Cryptography) in sensor networks. Security Mechanism is at two levels these are high level and low level mechanism.

1. **High Level Security**
   i. SGM (Secure Group Management)
   ii. ID (Intrusion Detection)
   iii. SDA (Secure Data Aggregation)
2. **Low Level Security**
   i. Robustness to Communication DoS
   ii. Security Routing
   iii. Resilience to Node Capture
   iv. Key Establishment and trust setup
   v. Security and Authentication
   vi. Privacy

SECURITY PROTOCOLS IN SENSOR NETWORKS

Cryptography is a basic technique to achieve the security in a network. This establishes a secure relationship between two end points. In this, sender encrypts the original data and receiver decrypts the received data to obtain an original data. Different types of keys are used in the process of cryptography. The various protocols that are proposed by different authors for solving the security issue in WSN are:

1. SPINs

SPIN (Sensor Protocols for Information via Negotiation) protocol works in three steps. First, a node advertises the ADV packet containing the metadata. If the received node is interested in the data then it sends the request for data using REQ packet. Finally, the advertiser node after receiving request sends the DATA packet to the requestor node. It performs best in small size networks because of its efficiency and high latency properties. Typical SPIN consists of two secure building blocks named as μTESLA (Timed Efficient Stream Loss-tolerant Authentication) and SNEP (Sensor Network Encryption Protocol). SNEP provides confidentiality, authentication and integrity. It uses the concept of encryption. To authenticate the data, MAC (Message authentication Code) is used. It adds 8 bytes to the message. To reduce the communication overhead, SNEP uses a shared counter between sender node and receiver node. After each block counter gets incremented. Counter helps in identifying the freshness of data. In TESLA, digital signatures are used to authenticate the data packet. Sink node computes a MAC on the packet after receiving the packet with the secret key to send an authenticated packet back to source. After receiving a packet node confirms that the sink does not disclose the computed MAC key to other nodes. With this, receiving node assures that data packet is original and no alterations are done in the packet.

2. LEAP

LEAP (Localized Encryption and Authentication Protocol) is a protocol with key management scheme that is very efficient with its security mechanisms used for large scale distributed sensor networks. It generally supports for inside network processing such as data aggregation. In-network processing results in reduction of the energy consumption in network. To provide the confidentiality and authentication to the data packet, LEAP uses multiple keys mechanism. For each node four keys are used known as individual, pair wise, cluster and group key. All are symmetric keys and use as follows: Individual Key: It is the unique key used for the communication between source node and the sink node.

i. **Pair wise Key:** It is shared with another sensor nodes.
ii. **Cluster Key:** It is used for locally broadcast messages and shares it between the node and all its surrounding neighboring nodes.
iii. **Group Key:** globally shared key used by the entire network Nodes. These keys can also be used by other non-secured protocols to increase the network security. LEAP is satisfies several security and performance requirements of WSN. LEAP is used to defend against HELLO Floods Attack, Sybil Attack and Wormhole Attack.

3. TINYSEC

TINYSEC is link layer security architecture for WSNs. It is a lightweight protocol. It supports integrity, confidentiality and authentication. To achieve confidentiality, encryption is done by using CBC (Cipher-block chaining) mode with cipher text stealing, and authentication is done using CBC-MAC. No counters are used in TINYSEC. Hence,

it doesn't check the data freshness. Authorized senders and receivers share a secret key to compute a MAC. TINYSEC has two different security options. One is for authenticated and encrypted messages (TinySec-AE) and another is for authenticated messages (TinySec-Auth). In TinySec-AE, the data payload is encrypted and the received data packet is authenticated with a MAC. In TinySec-Auth mode, the entire packet is authenticated with a MAC, but on the other hand the data payload is not encrypted. In CBC, Initialization Vector (IV) is used to achieve semantic security. Some of the messages are same with only little variation. In that case IV adds the variation to the encrypted process. To decrypt the message receiver must use the IV. IV sare not secret and are included in the same packet with the encrypted data.

4. **ZIGBEE**

ZIGBEE is a typical wireless communication technology. It is used in various applications such as military security, home automation and environment monitoring. IEEE 802.15.4 is a standard used for ZIGBEE. It supports data confidentiality and integrity. To implement the security mechanism ZIGBEE uses 128 bit keys. A trust center is used in ZIGBEE which authenticates and allows other devices/nodes to join the network and also distribute the keys. Generally, ZIGBEE coordinator performs this function. Three different roles in ZIGBEE are:

i. **Trust Manager:** It authenticates the devices which are requesting to join the network.
ii. **Network Manager:** It manages the network keys and helps to maintain and distribute the network keys.
iii. **Configuration Manager:** It configures the security mechanism and enables end-to-end security between devices.

CHALLENGES

WSNs endure many restrictions like little computation capability, limitedmemory, less energy resources, propensity to physical capture, and deficient of infrastructure, which make them open to many security attacks or challenges and make security techniques inevitable and desirable with some security solutions. All the security mechanisms discussed in the previous section provide security to WSNs to a certain level only. There are still remaining many issues and challenges which need to be addressed and resolved. It has been deduced that there are still many issues remaining which need to be addressed to make WSNs secure and efficient like:

- Public Key cryptography methods require excessive computation and storage in resources constrained WSN.
- Most of the security techniques are specific to certain attack which needs to be flexible.
- Key distribution problem need to be addressed to achieve encrypted and secure communication.
- Key Updating is an open issue.
- Key Revocation is needs to be addressed to prevent the malicious node from participating in normal communication

The computational overhead need to be reduced in resource constraint environment of WSN. The scalability is also desired to make the WSNs flexible for node addition and deletion.

CONCLUSION

Wireless Sensor Network has an great significance in all aspects military and civilian but it needs protection from all kinds security threats and attacks. Today's most of the offered security mechanisms are based on definite network model or specific attack as there is no such combined or general model to make certain overall security. To combine the different security techniques together to work in collaboration with each other will lay researchers open to a tough challenge. It will be also important to notice the adaptability, cost-effectiveness and energy efficiency to deploy such schemes in different applications of WSNs.

REFERENCES

1. Jun Wu, Kaoru Ota, Mianxiong Dong, Chunxiao Li, "A Hierarchical Security Framework for Defending Against Sophisticated Attacks on Wireless Sensor Networks in Smart Cities", IEEE Access, Vol. 4, pp. 416-424, 2016.
2. Agnihotri, Ram Bhushan, Ajay Vikram Singh, and Shekhar Verma. "Challenges in wireless sensor networks with different performance metrics in routing protocols." In Reliability, Infocom Technologies and

Optimization (ICRITO) (Trends and Future Directions), 2015 4th International Conference on, pp. 1- 5. IEEE, 2015.

3. Goutam Mali, Sudip Misra, "TRAST: Trust-Based Distributed Topology Management for Wireless Multimedia Sensor Networks", IEEE Transactions on Computers, Vol. 65, Issue: 6,pp. 1978-1991, 2015.
4. Said O. Amara, R. Beghdad and Mourad Oussalah, “Securing Wireless Sensor networks: A survey”,Taylor & Francis, 04 feb 2013.
5. Akyildiz, I. F., Su, W., Sankarasubramaniam, Y, and Cayirci, E., “Wireless Sensor Networks: A Survey”, Computer Networks, 38, 2002, pp. 393-422.
6. Culler, D. E and Hong, W., “Wireless Sensor Networks”, Communication of the ACM, Vol. 47, No. 6, June 2004.
7. Dai, S, Jing, X, and Li, L, “Research and analysis on routing protocols for wireless sensor networks”, Proc. International Conference on Communications, Circuits and Systems, Volume 1, 27-30 May, 2005, pp. 407-411.
8. Pathan, A-S. K., Islam, H. K., Sayeed, S. A., Ahmed, F. and Hong, C. S., “A Framework for Providing E-Services to the Rural Areas using Wireless Ad Hoc and Sensor Networks”, to appear in IEEE ICNEWS 2006.
9. Xiangwu Gong, Hang Long, Feihong Dong, Qing Yao, "Cooperative security communications design with imperfect channel state information in wireless sensor networks", IET Wireless Sensor Systems, Vol. 6, Issue: 2, pp. 35-41, 2016.
10. Y. Wang, G. Attebury, and B. Ramamurthy, “A Survey of Security Issues in Wireless Sensor Networks”, IEEE Commun. Surveys Tutorials, vol. 8, pp. 2–23, year 2006.
11. D. Estrin et al., “Instrumenting the World with Wireless Sensor Networks,” Proc. Int’l. Conf. Acoustics, Speech and Signal Pro- cessing, Salt Lake City, UT, May 2001.