International
Journal
Of Advanced Research in Engineering & Management (IJAREM)
ISSN: 2456-2033 || PP. 43-49

Wireless Sensor Network Security on Air: Issues and Challenges – A Review

[1]Yesodha.P, [2]S.Prithi, [3]G. Jenny Niveditha
[1,2,3]*Assistant Professor, Department of Electronics & Communication Engineering*
[1,2,3]*Prince Shri Venkateshwara Padmavathy Engineering College, Chennai – 600 127, Tamil Nadu.*

Abstract: Wireless networking is grown from cellular voice telephony to wireless access to internet. After a decade of exponential growth, today's wireless industry is one of the largest industry in the world. The sensors with actuators and general purpose computing elements, can act as nodes for communicating information through wireless medium and many sensors can be linked together to form a network called Wireless Sensor Network. Wireless sensor networks consist of tiny sensors to monitor environmental conditions such as temperature, pressure, vibration, motion or pollutant. The sensors are deployed in environment for commercial, military and civil applications. This paper reviews about the concept of wireless sensor network, types of attack on WSN, security issues and challenges experienced by such networks.

Keywords: Wireless Sensor Network (WSN), Sensor Nodes, Attacks, Security, Challenges and applications.

I. Introduction

The wireless technology is emerging as a recent trend in communication. Today, the wireless industry grown ahead than wired industry. The main sources of information such as voice, data and video are transmitted through wireless telecommunication devices. The data oriented wireless networks are divided into the wide area wireless data, local broadband and ad hoc networks.

Wired and Wireless /medium:

Wired medium provides a reliable, guided link that conducts an electrical signal from one terminal to another. Compared with wired media, wireless medium is unreliable, has low bandwidth and it is of broadcast nature.

Wired media provide us an easy way to increase capacity, whereas with a wireless medium, we are restricted to limited band for operation.

II. Wireless Sensor Networks

The wireless sensor network consist of large number of sensor nodes. The nodes contain tiny sensors with actuators with general purpose computing elements. These nodes are densely deployed either inside the phenomenon of interest or very close to it. Sensor nodes are small, low-cost, low-power devices that have following functionality:

- ☐ Communicate on short distances
- ☐ Sense environmental data
- ☐ Perform limited data processing

The sensors used in sensor fields are dependent on the application of the specific wireless sensor network. Some of the sensors used in WSN are vibration sensors, fire sensors, humidity sensors, light sensors and proximity sensors to calculate location.

Network usually also contains "sink" node which connects it to the outside world.

International
Journal
Of Advanced Research in Engineering & Management (IJAREM)
ISSN: 2456-2033 || PP. 43-49

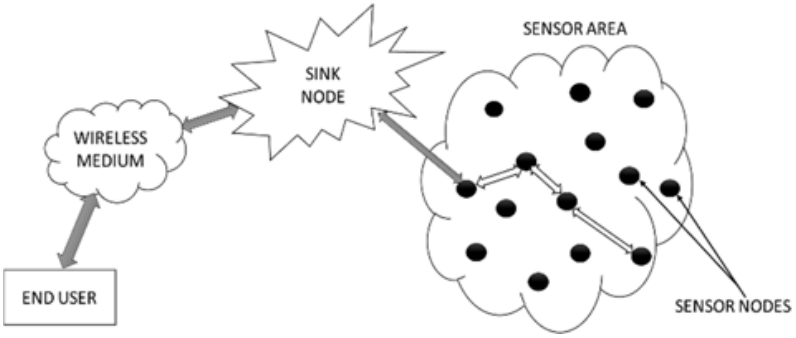

Fig. 1 Wireless Sensor Network

The sink node establishes a communication link between the sensor field and users at the outside world. The sink node act as a data collection agent from the sensor nodes.

The sensor nodes can also be connected in multihop configuration. In such configuration, some of the sensor nodes act as base station to collect information and regenerate them faithfully to ensure successful transmission.

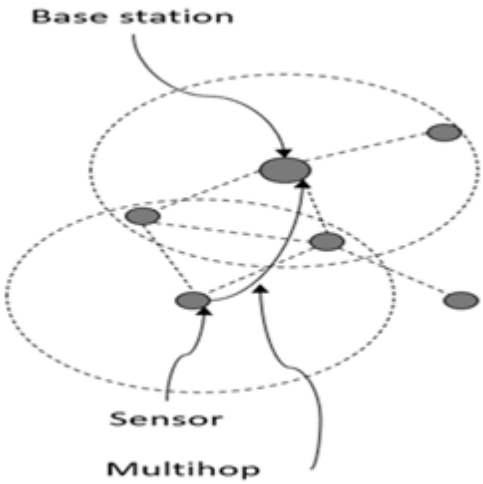

Fig. 2 Sensor nodes in Multihop configuration

In multihop configuration, the messages takes many number of hops before reaching the actual destination. Here, more than one node act as an intermediate node.

Factors influencing sensor network design

While designing a wireless sensor network, the following factors must be considered.

- **Fault tolerance:** Fault tolerance is the ability to sustain sensor network functionalities without any interruption due to sensor node failures. The fault tolerance level depends on the application of the sensor networks.
- **Scalability:** Scalability measures the density of the sensor nodes. The number of nodes to be deployed in the
- environment must be considered before the network design.
- **Production costs:** The cost of a single node is very important to justify the overall cost of the networks.
- **Transmission media:** In a multihop sensor network, communicating nodes are linked by a wireless medium. To enable global operation, the chosen transmission medium must be available worldwide. For example, the transmission medias can be used are Radio, Infrared and optical media.

Physical limitations

The physical limitations of wireless sensor networks are – limited battery power supply for the sensor nodes, energy consumption, memory size and communication bandwidth.

Characteristics

i) Ad-hoc Deployment: Sensor nodes are randomly deployed to the environment without any topology, the individual nodes will identify their connectivity and distribution between nodes by broadcasting an identity packets.
ii) Fault Tolerance: The sensor node may fail due to physical damage or lack of energy.
iii) Scalability: The number of nodes deployed are in terms of hundred, the wireless network protocol should update the information about the nodes during inclusion and deletion of nodes.
iv) Quality of service: The quality of service depends on presence of real-time nodes.

III. Security And Attacks

Security Primitives

The primary requirement for designing a sensor network architecture are

- **Confidentiality**
  The node should have ability to conceal message from a passive attacker
- **Integrity**
  The Node needs an ability to confirm the message has not been tampered.
- **Authentication**
  The nodes should ensure that the messages are from the nearby node which is present in the network.
- **Access Control**
  The Node should have the ability to determine if a node is authenticated to use the resources.

The main security threats in wireless sensor networks are,

- Radio links are insecure – eavesdropping / injecting faulty information is possible.
- Sensor nodes are not temper resistant – if it is compromised, attacker obtains all security information.

The different types of attack that the wireless sensor network experiences are

Attacks

The wireless sensor networks can be attacked by the attackers to illegally obtain keys stored in the nodes. The following are some of the examples of attacks given to a wireless sensor network.

i) Hello flood attack:

In many WSN routing protocol, the nodes are expected to broadcast HELLO packets after deployment to discover the neighbouring packets. In HELLO flood attack, the node will broadcast information with a huge signal strength, so that all the other nodes think that they are close to the broadcast node.

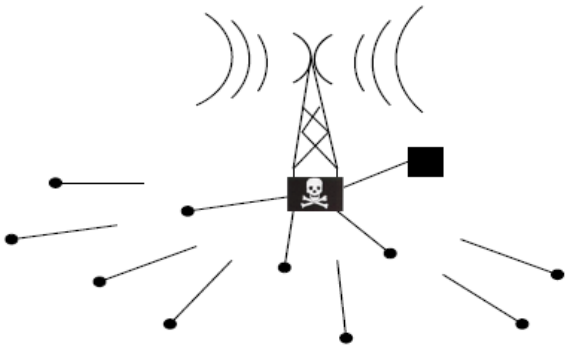

Fig. 3 Example of hello flood attack

ii) Wormhole attack:

In this type of attack, nodes are transmitted from one part of the network and the reply will be received from other part of the network.

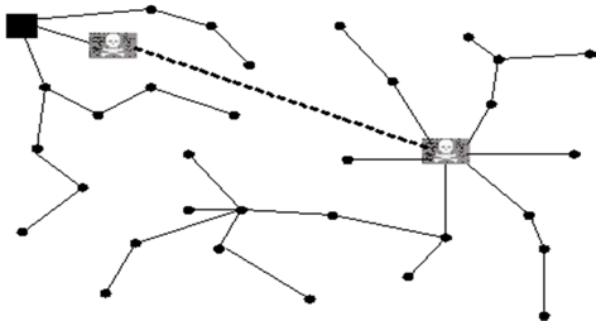

Fig. 4 Example of warm-hole attack

The well placed wormhole can completely rearrange the order of routing nodes. Wormholes attract the distant nodes that are close to the sink. This may lead to sinkhole attack if the node advertises high–quality sink route to the sink. Wormholes may convince two nodes that they are neighbours when on fact they are far away from each other.

iii) Acknowledgment spoofing attack:

In the routing protocols of wireless sensor network, link layer acknowledgements are expected after transmission of packets. In this attack, the attacker may spoof acknowledgement and convince the node that, weak link is strong or the dead node as alive. Consequently weak link may be selected for routing and the packets sent through that link may be lost or corrupted.

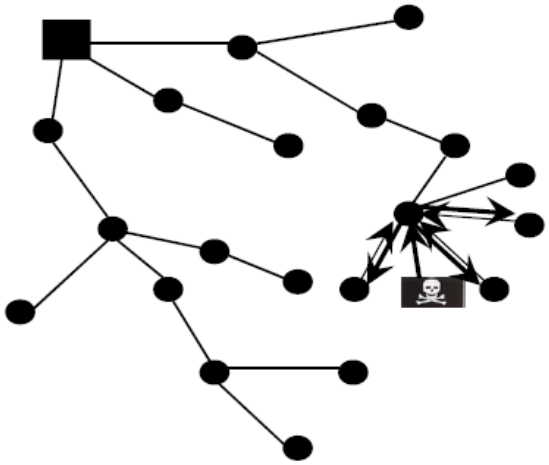

Fig 5. Representation of Acknowledgment spoofing attack

iv) Selective forwarding:

In multihop scheme, the nodes are expected to forward received packets faithfully. But sometimes, the nodes are refused to resend the all received packets, only few packets will be forwarded.

Fig. 6 Selective Forwarding algorithm

v) Sinkhole attack:

The attacker creates a sinkhole by advertising high quality route to a base station. Due to this, all nodes are connected to real sink and the packets will be discarded. Here almost all traffic are directed to false sinkhole.

vi) Sybil attack:

In this type of attack, a single node pretends to be present in different parts of the network. This attack affects routing protocol of the network.

IV. Challenges In Security

The following are some of the challenges to be considered while planning security.

- ☐ When using cryptography technique, complex key management should be avoided.
- ☐ Packet overhead must be reduced. One method for reducing packet overhead is to discard the packets with a destination address which is not same as their own address.

Key Management

The protocol must establish a key between all sensor nodes that must exchange data securely. Key is used to support Node addition / deletion. It should work in undefined deployment environment. Unauthorized nodes should not be allowed to establish communication with network nodes.

Sensor devices have limited computational power, making public-key cryptographic primitives too expensive in terms of system overhead.

- ☐ The simplest solution is a network-wide shared key. The problem is that, if even a single node were compromised, the secret key would be revealed, and decryption of all network traffic would be possible.
- ☐ Then better solution is to use a single shared key to establish a set of link keys, one per pair of communicating nodes, then erase the network-wide key. The problem is that, it does not allow addition of new nodes after initial deployment.
- ☐ Bootstrapping the keys using a trusted base station is another solution for key management. Each node needs to share only a single key with the base station and set up keys with other nodes through the base station. The base station becomes a single point of failure, but being that there is only one base station, it becomes feasible (financially and otherwise) to utilize tamper-resistant packaging for the base station, reducing the threat of physical attack.

Key calculation

In many WSN protocol, the use of secret key is required at different nodes to prevent attacks. The keys are required at

- ☐ Base station to node key calculation
- ☐ Nodes to cluster leader key calculation
- ☐ Cluster leader to cluster leader key calculation

- ☐ Cluster leader to base station key calculation

Key Management: Constraints

The following are the constraints to be considered for key management.

1) Sensor node constraints:

- ☐ Battery power
- ☐ Computational energy consumption
- ☐ Communication energy consumption
- ☐ Transmission range
- ☐ Memory
- ☐ Temper protection
- ☐ Sleep pattern

2) Network constraints:

- ☐ Ad-hoc network nature
- ☐ Packet size

Key revocation

Key revocation is another method increase security level in data transmission through wireless sensor networks. This can be accomplished in the following way:

- ☐ A controller node that has all keys and ids in its memory, broadcasts a message containing a list of k key identifiers for the key ring to be revoked.
- ☐ This message is signed with signature key which is encrypted and unicasted to all nodes prior revocation. This encryption is done using individually shared between node and controller keys.
- ☐ After obtaining a signature key, each node locate received identifiers in its key ring and removes the corresponding keys if they are present.
- ☐ Since some links might disappear they should be reestablished using keys that are left in the key ring.

V. WSN Applications

WSN can be used to monitor the conditions of various objects or processes. Some examples:

- ☐ Military: Friendly forces monitoring, battlefield surveillance, biological attack detection, targeting, battle damage assessment, Enemy movement (tanks, soldiers, terrorists etc).
- ☐ Ecological: Fire detection, flood detection, agricultural uses.
- ☐ Health related: Human physiological data monitoring.
- ☐ Miscellaneous: Car theft detection, inventory control, habitat monitoring, home applications

VI. Conclusion

Ensuring security in wireless sensor network requires encryption, key management and key revocation techniques. Link layer encryption prevents majority of attacks: bogus routing information, Sybil attacks, acknowledgment spoofing, etc. This makes the development of an appropriate key management architecture a task of a great importance.

Wormhole attack, HELLO flood attacks and some others are still possible: attacker can tunnel legitimate packets to the other part of the network or broadcast large number of HELLO packets. Multi path routing, bidirectional link verification can also be used to prevent particular types of attacks like selective forwarding, HELLO flood etc. Thus, security solutions are adaptive based on the nature of attacks.

VII. References

[1]. Raja Waseem Anwar, Majid Bakhtiari, Anazida Zainal, "Security Issues and Attacks in Wireless Sensor Network", World Applied Sciences Journal 30 (10): 1224- 1227, 2014 ISSN 1818-4952.

[2]. Pooja, M. and D.Y. Singh, 2013. Security Issues andSybil Attack in Wireless Sensor Networks, International Journal of P2P Network Trends and technology.

[3]. Jain, M.K., 2011. Wireless sensor networks: Security issues and challenges. International Journal of Computer and Information Technology

[4]. Mahmood, Ahmed R., Hussein H. Aly, and Mohamed N. ElDerini (2011), Defending against energy efficient link layer jamming denial of service attack in wireless sensor networks, In Computer Systems and Applications (AICCSA), 2011 9th IEEE/ACS International Conference on, pp. 38-45. IEEE.

[5]. LuisJaveir Garcia Villalba, Ana Lucila Sandoval Orozco, Alicia TrivinoCabera and Claudia JacyBarenco Abbas, "routing Protocols in Wireless Sensor Networks," Sensors2009.

[6]. Kalita, H.K. and A. Kar, 2009. Wireless sensor network security analysis. International Journal of Next- Generation Networks (IJNGN), 1(1): 1-10.

[7]. Shi, E. and A. Perrig, 2006. Designing secure sensor networks. IEEE Wireless Commun., 11: 38-43. DOI: 10.1109/MWC.2004.1368895.