Sensor Network Security Issues In Each Layer

Jaykumar Shantilal Patel
Chaudhari Technical Institute, MCA Department, Opp. S. T. Bus Depot,
Sector-7, Gandhinagar, (Gujarat-INDIA).
E-mail: jay_sp_mca@yahoo.co.in

Dr. Vijaykumar M. Chavda
N. P. College of Computer Studies and Management - Kadi (Gujarat-INDIA)
E-mail: dr.vijaychavda@gmail.com

Abstract:

Sensor network is an amalgamation of hundreds or thousands of sensor nodes. These nodes have sensing, computing and processing potentiality. The sensor network is generally deployed in the hostile environment where the security is very essential. Nowadays security is an important issue in almost every network. Sensor network bears from many constraints like computational potentiality, limited memory, limited energy, limited resources, vulnerability to physical capture etc. These constraint based sensor network makes security as a challenging task. The various attacks at each layer are usual. Resource limitations nature of sensor network makes these attacks even more dangerous. The paper concern the various attacks at each layer in layer architecture of sensor network protocol stack.

Keyword: Sensor network Security, Layer architecture, Attacks.

1. Introduction:

Sensor network is a combination of hundreds or thousands of sensor nodes which having very limited resources, where the attacker may have very powerful resources having extremely long range communication capability. Therefore to maintain security in sensor network is a foremost issue. The traditional security mechanism of normal computer network may not directly shift to the sensor network because of the resource constraint nature of the nodes. Information security is the hot topic of research for decades to deal the prevailing security requirements [1]. In wireless network the packet must be lightweight, due to that it takes a large amount of time to transmit large file [2]. As the Internet and other forms of electronic communication become more prevalent, electronic security is becoming increasingly important [3]. The future work in the design of energy-efficient broadcast routing protocols in wireless should try to reduce the transmission redundancy and overall network overhead, and thus achieve the minimum energy consumption and the maximum network lifetime [2]. The fast progression of data exchange in electronic way, information security is becoming more important in data storage and transmission [1]. The algorithm is enriched with various calculations through which the cipher text becomes unpredictable and breaking the security by eavesdropper becomes harder [3].

2. Layer architecture of sensor network:

Sensor network have five different layers through which the communication is establish. The Layer is: Application layer, Transport layer, Network layer, Data-link layer and Physical layer. Figure-1 shows the layer architecture of sensor network.

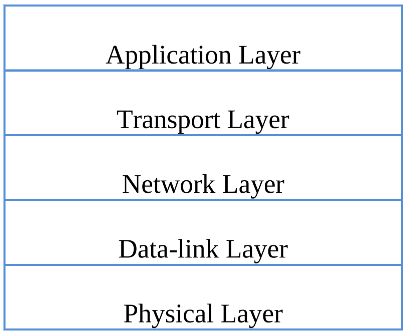

Figure: 1 - Sensor network Layer Architecture.

3. Layer based attacks in sensor network:

Table-1 shows the layer based attacks and the protocol implementation at each layer.

Layer Name	Attacks	Protocol
Application Layer	Attacks on reality	BOOTP, DHCP, DNS, HTTP, POP3, SSH, Telnet
Transport Layer	Flooding, Injecting false messages (data integrity attack), Energy drain attacks, De-synchronization	TCP, UDP, SPX
Network Layer	Spoofing, Selective forwarding or black holes, Sinkholes, Sybil attacks, Wormholes, Acknowledgement spoofing, Hello Flood attacks	RIP, OSPF, EGP, IPX, IPV6, ARP
Data-Link Layer	Collision	Frame Relay, FDDI, Ethernet
Physical Layer	Jamming, Tampering	Sonet, ISDN, SDH

Table: 1- Security attacks on specific layer with protocol implementation

4. Application Layer

The objective of Application Layer is to present final output by ensuring smooth information flow to lower layers, this layer is responsible for data collection, management and processing of the data through the application software for getting reliable results [4]. The numbers of attacks are there among the several attacks the attacks on reality is the most common attack at application layer. The task performance at application layer covers: to support various applications like data aggregation application, attributes based clustering application, location tracking application, time synchronization application, turning sensor node on or off application, configuration and re-configuration application, security application etc. Among these various applications recently the security in senor network has attracted the more attentions of researcher. The security application mainly covered the confidentiality and authenticity aspect in sensor network. The secure key distribution and secure data communication is the core of the security implementation in sensor network.

4.1 Attacks on reality: The attack on reality is actually the attack on authenticity of data. Adversary access data from the one path during the communication modify the data and then transmit the altered data to the actual recipient. When the actual recipient received data, the data is not real. Means it is attack on the reality of the data being transmitted. These kinds of attacks may lead to more energy consumption and hence energy drains attack. Usually to ensure reliability acknowledgement is expected for each successful data delivery [5].

5. Transport Layer

The objective of Transport Layer is to establish communication for external networks using either TCP protocol or UDP protocol. Generally the TCP protocol is more popularly used. Depending on the application the relevant protocol is selected for the implementation. Sometimes the attacker might be strong enough to reach up to the transport layer, due to the attack being undetected at the lower layers [4]. The transport layer helps to maintain the flow of data if the sensor networks application requires it [6]. The transport layer attacks are: Flooding, Injecting false messages (data integrity attack), Energy drain attacks and De-synchronization.

5.1 Flooding: Sometimes the malicious node can cause immense traffic of useless messages on the network. This is known as the flooding [4]. The malicious node generates the dummy packet and sends across the network that can lead to network traffic. This can cause to the congestion. Flooding is a one kind of Denial-of-service attack. One possible solution to deal with the malicious packets is to introduce the authentication mechanism at every node end. So that before accepting the packet every node checks its authenticity, if packet coming from the authorized node it will be accepted either it will just ignore. This authentication mechanism can introduce using identity verification through trust based station.

5.2 Injecting false messages – data integrity attack: The goals of this attack are to falsify sensor data and by doing so compromise the victim’s research [4]. It is also a type of Denial-of-service attack. It disrupts the sensor network routine operation so it will become worthless. This kind of attack can be resolved using encryption mechanism or introducing digital signature. The encryption mechanism covers symmetric and asymmetric approach for implementation. The asymmetric approach gives better security than symmetric but this requires a lot of additional computational as we as communication overhead.

5.3 Energy drain attacks: sensor networks are battery operated and having limited life time. It is very difficult to replace the nodes batteries or to recharge the nodes batteries. Adversary creates a fabricated message to generate large amount of traffic across the network. The adversary node continuously transmits the packets across the network that may lead to the energy consumption of the node. The aim of this attack is to destroy the sensor nodes from the network, degrade performance of the network and ultimately split the network grid and consequently take control of part of the sensor network by inserting a new Sink node [5]. To minimize the damage caused by this attack fabricated reports should be dropped en-route as early as possible [4].

5.4 De-synchronization: This attack tries to disturb an existing connection. An adversary continuously swindles packets to an end host. This host then demands retransmission of dropped frames and hence the energy of nodes is wasted, therefore degrading the performance of the whole network [7].

6. Network Layer

The objective of Network layer is to find best path for efficient routing mechanism. This layer is responsible for routing the data from node to node, node to sink, node to base station, node to cluster head and vice versa [4]. Routing protocol should be responsible for preventing eavesdropping [8]. In sensor network, network layer is vulnerable to various attacks. Broadly, they are categorized in two types [9]. ***Passive attack***- An adversary can only discover information without modifying them. It is difficult to detect these attacks. ***Active attack***- An adversary can modify/falsify/change/alter the information and thus interfere in functioning of the network. Network layer is responsible for specifying the assignment of addresses and how packets are forwarded [10].

6.1 Spoofing: In spoofing attack one person or node or programme mask as another person or node or program. Hence it can have fake communication over the sensor network that can gain illegitimate advantage. Spoofing attack affect the network traffic. It can lead to the packet loss scenario that can lead to retransmission cause into high communication overhead across the sensor network. Sometime small broadcast messages capture by malicious node and retransmit other broadcast afterwards.

6.2 Selective forwarding or black holes: When data is transmitted from source to destination in sensor network, it is based on hope-by-hope communication rules. So, the sensors pass information from one end to the base station by routing them through intermediate nodes [4]. Sometimes a malicious node may be present within the network path. In a flooding based protocol, the attacker (malicious node) listens to requests for routes then replies to the target nodes that it contains the high quality or shortest path to the base station [11]. The result of selective forwarding is the loss of large amount of data during the communication. In another case it may happen that the malicious node drops all the packets it receives, hence no information is forwarded. This creates a black hole [4].

6.3 Sinkholes: In this attack the attacker lures most of the sensor network traffic to pass through the malicious node thus creating a sinkhole with malicious node at its centre [6]. Since the most of the data passes through the malicious node, the malicious node can do anything with the data passes through. The major chance is eavesdropping.

6.4 Sybil Attacks: An adversary node assumes identity of multiple nodes means the node having multiple identities. In sensor network the authorized real node only have its own single identity. Hence, by the wrong multiple identity nodes send and receive the data packet across the network that can lead to falsie communication at authorized node end. This kind of attack may cause the falsification of routing mechanism as well as the falsification of the resource assignment.

6.5 Wormholes: malicious nodes may create the hidden channel between them known as wormhole. The malicious node may receive the packets from the one section of the network while it transmit into other section of the network this will create the network congestion through misguiding the network traffic into single direction. This will create the fake scenario. This may lead to retransmission and resulting into more energy consumption. In some cases the sinkhole by attracting it neighbour.

6.6 Acknowledgment Spoofing: Routing algorithms used in the sensor network environment are mostly based on acknowledgement. An adversary can spoof the acknowledgement to provide the false information to the sending end. Example, when a node is actually died but spoofed acknowledgement for that node misguides that node is still alive.

6.7 Hello Flood Attacks: HELLO packet is used to check the neighbour through specified radio range. Attacker used the high power radio range to shows up it as neighbour of multiple node location. Attacker broadcast the HELLO packet to pretend its identity as neighbour. So, the real nodes misguide and compromised with the falsie attacker node.

7. Data-link Layer

The main objective of the data link layer is to provide surety for interpretability amongst the communication between node ends. It is also responsible to maintain the error detection as well as error correction mechanism. Among the numbers of error detection and error correction mechanism, the light weighted and efficient mechanisms are selected for the implementation.

7.1 Collision: in sensor network it may happen that when one node wants to transmit, the channel was currently occupied by the other one. So, node has to wait until and unless the channel will became free. If carrier sense is not introduced it may result into collision. When the collision occur the retransmission is required, that lead to high communication overhead across the sensor network.

8. Physical Layer

The physical layer addresses the needs of a simple but robust modulation, transmission and receiving techniques. [6]

8.1 Jamming: Radio signals used for the data communication may interference with the other radio frequencies of sensor network known as jamming situation. When adversary introduces it utilize the high radio frequencies that lead the interference to actual radio communication across the network. It is also a one part of the denial-of-service attack at the physical layer. Hence the fair communication may not be possible and it blocks some node.

8.2 Tampering: Sometimes the authorize node tampered by the adversary. Such situation called the tampering. Tempering attack may damage the physical characteristics of the specified node. Generally it affects the sensing capacity of the node in term of the radio frequencies like spread spectrum and frequency hopping.

9. Conclusion

In this paper we present the brief summary of sensor network, layer architecture of sensor network and the layer based attack in the sensor network. This paper gives an idea of a major subset of security problems that Wireless Sensor Network faces because of its outstanding design characteristics, communication and deployment pattern. Providing security in a wireless sensor network is a challenging task. We have discussed various security attacks present at each layer of sensor network protocol stack. Most of the researchers are busy in developing the security mechanism for each layer of the sensor network protocol stack shown in Figure-1.

10. References:

[1] N. Sethi and D. Sharma, “A novel method of image encryption using logistic mapping”, International Journal of Computer Science Engineering (IJCSE), ISSN: 2319-7323, Vol. 1 No.02 November 2012.

[2] M. Dinesh and E. M. Redddy, “Ultimate Video Spreading With Qos over Wireless Network Using Selective Repeat Algorithm”, International Journal of Computer Science Engineering (IJCSE), ISSN: 2319-7323, Vol. 2 No.04, July 2013.

[3] S. Karmakar and S. Chandra, “An Approach for Ensuring Security and its Verification”, International Journal of Computer Science Engineering (IJCSE)”, ISSN: 2319-7323, Vol. 2 No.03 May 2013.

[4] A. S. Sastry, S. Sulthana and Dr. S. Vagdevi, “Security Threats in Wireless Sensor Networks in Each Layer”, International Journal Advanced Networking and Applications, ISSN: 0975-0290, Volume: 04, Issue: 04, Pages: 1657-1661, 2013.

[5] P. mohanty, S. Panigrahi, N. sarma and S. satapathy “Security issues in wireless sensor network data gathering protocols: a survey” Journal of Theoretical and Applied Information Technology, 2005.

[6] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam and E. Cayirci, “Wireless sensor networks: a survey”, Computer Networks, Page: 393–422, Published by Elsevier, 2002.

[7] A. Singla and R. Sachdeva, “Review on Security Issues and Attacks in Wireless Sensor Networks”, International Journal of Advanced Research in Computer Science and Software Engineering, ISSN: 2277 128X, Volume 3, Issue 4, April 2013.

[8] P. Barua and S. Indora, “Overview of Security Threats in WSN”, International Journal of Computer Science and Mobile Computing, ISSN 2320–088X, Vol. 2, Issue. 7, page: 422 – 426, July 2013.

[9] H. Modares, R. Salleh and A. Moravejosharieh, “Overview of Security Issues in Wireless Sensor Networks”, Modelling and Simulation, Third International Conference on Computational Intelligence, 2011.

[10] Y. Wang, G. Attebury and B. Ramamurthy, “A Survey of Security Issues In Wireless Sensor Networks”, IEEE Communications Surveys & Tutorials, Volume 8, No. 2, 2nd Quarter, 2006.

[11] A. Pathan, H.Lee and C. Hong, “Security in Wireless Sensor Networks: Issues and Challenges”, ICACT, ISBN 89-5519-129-4, Feb. 20-22, ICACT-2006.