International Journal of Recent Trends in Engineering & Research
ISSN(ONLINE) : 2455-1457
IMPACT FACTOR : 3.344

A Survey on Wireless Sensor Network Security

Sonia[1], Kusum Dalal[2]
[1,] *M.Tech. Scholar, DCRUST Murthal, 131027, India*
[2]*Assistant Professor, DCRUST Murthal, 131027, India*

Abstract-This paper presents a brief overview on WSN (wireless sensor network) network architecture and also it presents a detailed discussion on various security goals related to sensor nodes in WSN network such as Data confidentiality, Data integrity, Availability, Authentication, Data freshness, Time Synchronization etc. Numbers of hazardous attacks that can occur in a WSN network are presented in this paper for which solutions can be designed in order to improve the services of such networks. Such malicious attacks are as follows: Spoofed, altered, or replayed information, Selective forwarding, Sinkhole attack, Sybil Attack, HELLO flood attack, Wormholes Attack.
Keywords: Wireless sensor network, Attacks, Security issues, Sinkhole attack.

I. INTRODUCTION

"A sensor network is a deployment of massive numbers of small, inexpensive, self powered devices that can sense, compute, and communicate with other devices for the purpose of gathering local information to make global decisions about a physical environment" [1].

The sensors nodes are used for monitoring different environments in the cooperative manner and compute the data for analyzing. The two components of wireless sensor network aggregation and base station, aggregation collect the information from there nearby sensors, integrate them and send to the base station for processing. These sensor nodes consists of some major components sensing, processing after that communication [2]

The characteristics of WSNs are wireless medium, low power consumption, low cost and low data rate. Other characteristics of WSN are large numbers of sensors, collaborative signal processing, easily deployed, self-configurable and self-organize, and infrastructure-less. [3]

Wireless sensor network architecture:
Sensor Nodes: Sensors nodes are the heart of the network. They are in-charge of collecting data and routing this information back to a sink.
Gateway/Sink: A gateway enable to the communication between the sensor nodes (Field devices).The gateway are also called access points.

Task manager: A task manager is managing the operation, administration, security, and maintenance of all sensor nodes in a network.
Security manager: the security manager is responsible for the security of nodes in a network and management of keys.[4]. For example see Fig.1.

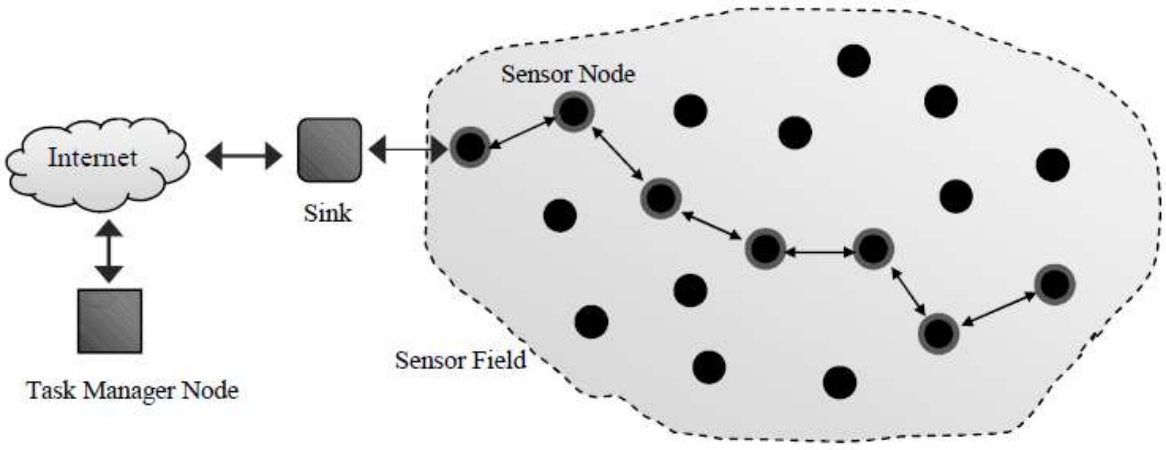

Fig. 1: Architecture of WSN

The remainder of the paper is organized as follows. In section 2, present the security requirements in WSNs. Section 3, present the previous work done Section 4, possible attack in wireless sensor network are discussed. Section 5, present the conclusion.

II. Goals

Security Goals in WSNs: The security services in a WSN should protect the information communicated over the network and the resources from attacks and misbehaviour of nodes. The most important security requirements in WSN are listed below:

2.1 Data confidentiality: It means restricting data access to authorized personnel. The data should not be leaked across adjacent sensor networks. It ensures that a given message cannot be understood by anyone other than the desired recipient.

2.2 Data integrity: Data integrity ensures that the receiver receives unaltered data in transit by any unauthorized personnel.

2.3 Availability: It ensures that the desired network services are available even in the presence of denial of service attacks.

2.4 Authentication: It ensures that the communication from one node to another node is genuine, i.e., a malicious node cannot masquerade as a trusted network node.

2.5 Data freshness: Data freshness ensures that the recent data is available without any replay of old messages by unauthorized personnel**.**

2.6 Self-organization: Nodes should be flexible enough to be self-organizing (autonomous) and self-healing (failure tolerant).

2.7 Robustness and survivability: Sensor network should be robust against the various attacks and if an attack succeeds, the impact should be minimized.

2.8 Time Synchronization: These protocols should not be manipulated to produce incorrect data.[5]

Constraints in wireless sensor network:[5]
Resource constraints: Sensor nodes have low computational capability in its limited resources, wireless communication bandwidth are limited, small memory etc.
Small message size: In sensor network are message size is small as compared to existing networks. There is no use of segmentation in many applications in wireless sensor network.

Sensor location and redundancy of data: In a sensor network are position of nodes is very important since data collection is normally based on location. Also there are use a common phenomenon to collect data, so these data are high probability then this data has some redundancy.

Cryptography:[7] Cryptography simply aims at making data not understandable to an unauthorized adversary which has the goal of data interpretation.

Plain Text The plain text is the actual message that has to be send to the other end.

Cipher Text: Cipher text is the original message is transformed into non readable message before the transmission of actual message.

Encryption: A process of converting Plain Text into Cipher Text is called as Encryption.

Decryption: It is a process of converting Cipher Text into Plain Text.

It consists of two categories.
1. Asymmetric Cryptography
2. Symmetric Cryptography.

Symmetric Cryptography:
Symmetric key cryptography mechanism use a single shared key between the two communicating host which is used both for encryption and decryption.

Asymmetric Cryptography: Asymmetric key cryptography also known as public key cryptography, which uses public-private pair key for encryption and decryption.

III. PREVIOUS WORK DONE

Raja waseem anwar et al. "Security Issues and Attacks in Wireless Sensor Network*"* This paper analyzed security issues and physical attacks. The most physical attacks disturb the wireless sensor network security goals like confidentiality, integrity, authenticity and availability.

Vikas kumar et al. "Wireless Sensor Networks: Security Issues, Challenges and Solutions" This paper presents the attacks and their classification in wireless sensor networks. Also it presents a brief overview of security mechanism and challenges of wireless sensor network.

Sahabul Alam et al. "Analysis of Security Threats in Wireless Sensor Network" This paper provides the Security schemes and the threat attacks in wireless sensor network. Security schemes like: Cryptography, Steganography and Physical layer Secure Access. Threat attacks like: Collisions, Tampering, Jamming, Unfairness, and Flooding etc. They also propose a solution for the attacks in wireless sensor network. One possible solution is the use of cryptography techniques.

Ritu Sharma et al. "Analysis of Security Protocols in Wireless Sensor Network" provides constraints, security goals, threat models and typical attacks on sensor networks and their defensive techniques or countermeasures relevant to the sensor networks, including security methods. Security goals in WSN :(Availability, Authorization, Authentication, Confidentiality etc).They also propose a solution for security in wireless sensor network and gives the overview of various security protocols.

Yih-Chun Hu et al. "Ariadne: A Secure On-Demand Routing Protocol for Ad Hoc Networks" ARIADNE is an on-demand secure ad hoc routing protocol based on DSR. It relies on highly efficient symmetric cryptography. It provides point-to-point authentication of a routing message using a message authentication code (MAC) and a shared key between the two parties. It copes with attacks performed by malicious nodes that modify and fabricate routing information with attacks using impersonation.

Abhishek Pandey et al. "A Survey on Wireless Sensor Networks Security" provide**s** the layered architecture of wireless sensor network**.** These are the different layer are different functions. The objective of Network layer is to find best path for efficient routing mechanism .In this layer are used leach protocol to save the energy consumption (power of sensor) so as to improve the life of sensors. LEACH gives cluster based transmission. The objective of application layer is responsible for data collection, management and processing of the data through the application software for getting reliable results. In this layer are used SPINS (security protocol in sensor network) protocol are provides data authentication.

Jyoti Attri et al. "Study on cryptographic techniques in computer network security" provide the overview of cryptography techniques like Symmetric and asymmetric key. In

symmetric key cryptography, single key is used for encryption and decryption process i.e. using same key data can be encrypted and decrypted **.**Symmetric key are very fast as compare to asymmetric key. Symmetric key is more sufficient for security in wireless sensor network.

IV. POSSIBLE ATTACKS IN WIRELESS SENSOR NETWORK ROUTING

4.1 Spoofed, altered, or replayed information

The most direct and most effective way of attacking any routing protocol is to target the information being exchanged between the nodes. By spoofing, altering or replaying routing information, adversaries can achieve a number of motives like creating routing loops, extending or shortening routing paths, attracting or repelling network traffic, increasing end- to-end latency, partitioning the network, generating false error messages, etc.

4.2 Selective forwarding

An honest node would always faithfully forward the received messages to its destination. However, a malicious node would refuse to forward certain messages and simply drop them, ensuring that the message doesn't reach the intended destination. This is called selective forwarding attack. A simple form of this attack is that the malicious node would act as a black-hole i.e. drops every message packet that arrives to it. But such nodes have the risk that the neighbouring nodes would consider them as dead nodes and would seek another route. So, adversaries adapt a more subtle form i.e. intelligently forward only certain messages. Hence, the risk of getting caught is minimized. Selective forwarding attacks are more effective when the attacker explicitly includes itself in the routing path of the data. Other ways of implementing selective forwarding is by jamming or causing collision on the transmitting information.

4.3 Sinkhole attack

In sinkhole attack, a compromised node is made to look very attractive to the surrounding nodes with respect to the routing algorithm. (For example, adversary can advertise a very high quality routing path and hence divert the path through it.) Hence a metaphorical sinkhole is created with the adversary at the centre. And now since the routing path is diverted through this adversary node, severe damages can be done by it. Sinkhole is a very effective way of implementing selective forwarding. Spoofing, altering or replaying the routing information can also be done by the adversary. The reason why sensor networks are highly susceptible to sinkhole attack is because all message packets being transmitted have a single ultimate destination, the base station. A compromised node only needs to provide a single high quality route to the base station and hence, effecting severe damages.

4.4 Sybil Attack

In Sybil attack, a single node presents multiple identities to the other nodes in the network. Routes believed to be passing through multiple nodes would actually be passing through the same adversary node and hence thereby running the risk of an endless loop.

Sybil stack pose significant threats to location-based routing protocol. Protocols which require exchange of location information would be adversely affected as adversary nodes, using Sybil attack, would be exchanging multiple sets of coordinates, rather than a single set of coordinates and hence can be in more than one place at a time.[6]

4.5 HELLO flood attack

Many protocols require broadcasting HELLO packets by the sensor nodes to announce it to the neighbours, thereby alerting them that it's within their transmission range. But an adversary could flood false HELLO packets. Hence, the nodes would consider it to be within the range while the adversary may be situated far from it. In such scenarios, nodes would be unnecessarily transmitting message and hence draining its energy. Protocols which depend upon exchange of location information between the nodes are likely to be targets of such attack.

4.6 Wormholes Attack

In wormhole attack, an adversary tunnels messages received in one part of the network over a low latency link and replays them in a different path. Wormhole attack normally involves two distant malicious nodes, misleading others to understate the distance between them by relaying packets along an outer channel, which is available only to the attacker. An attacker situated close to the base-station may completely disrupt the routing by creating a well-placed wormhole. This attack is likely to be used in combination with eavesdropping or selective forwarding. Detecting Wormhole attack is difficult when used along with Sybil attack. Wormholes can be intelligently used to create sinkholes

V. CONCLUSION

This paper presented a detailed picture about various security issues related to WSN networks. Also a brief introduction to cryptographic technique is made to enhance the security of wireless sensor network.

REFERENCES

1. Olariu S. et al., "Information assurance in wireless sensor networks", Sensor network research group, Old Dominion University.
2. *Raja Waseem Anwar, et al., "*Security Issues and Attacks in Wireless Sensor Network*",* World Applied Sciences Journal 30 (10): 1224-1227, 2014,ISSN 1818-4952
3. Sahabul Alam and Debashis De, "Analysis Of Security Threats In Wireless Sensor Network", International Journal of Wireless & Mobile Networks (IJWMN) Vol. 6, No. 2, April 2014
4. Vikash Kumar1. et al., " Wireless Sensor Networks: Security Issues, Challenges and Solutions", International Journal of Information & Computation Technology,ISSN 0974-2239 Volume 4, Number 8 (2014)
5. Yogesh Chaba. et al., "Analysis of Security Protocols in Wireless Sensor Network", Int. J. Advanced Networking and Applications 707 Volume: 02, Issue: 03, Pages: 707-713 (2010)
6. Sushma1.et al., "Security Threats in Wireless Sensor Networks'', IJCSMS International Journal of Computer Science & Management Studies, Vol. 11, Issue 01, May 2011 ISSN (Online): 2231 –5268
7. Jyoti Attri.et al., "Study on cryptographic techniques in computer network security'', Asian J.of Adv. Basic sci.: 2(3) , 98-102 ISSN (online):2347-4114
8. Sujesh P. Lal.et al., "Security Issues in Wireless Sensor Networks – An Overview'', Sujesh P. Lal et al, / (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 6 (1) ,

2015, 920-924
9. Jaydip Sen., "A Survey on Wireless Sensor Network Security'', International Journal of Communication Networks and Information Security (IJCNIS) Vol. 1, No. 2, August 2009
10. Abhishek Pandey. et al., "A Survey on Wireless Sensor Networks Security", International Journal of computer Application (0975-8887) Volume 3-No.2,June 2010
11. Wendi Rabiner Heinzelman.et al., "Energy-Efficient Communication Protocol for Wireless Microsensor Networks", International Conference on System Sciences, January 4-7, 2000, Maui, Hawaii.
12. David B. Johnson et al., "Ariadne: A Secure On-Demand Routing Protocol for Ad Hoc Networks", Wireless Networks 11, 21–38, 2005

