Review On Attacks & Countermeasures In Wireless Sensor Network

Dinesh Kumar Yadav, M. Tech Research Scholar

Department of Computer Science & Engineering, Geeta Institute Of Management & Technology, Kanipala, Kurukshetra
yadavnarpal56@hotmail.com

Ravi Kumar, Assistant Professor

Department of Computer Science & Engineering, Geeta Institute Of Management & Technology, Kanipala, Kurukshetra
ravi.kawatra@gmail.com

----------ABSTRACT----------

Wireless sensor networks are gettings significantly vital to many programs, and they were initially utilized by the military for surveillance functions. One of the important issues of WSNs is that they are very defenseless to protection threats. Due to the truth that these networks are susceptible to hackers; it is possible for one to enter and render a network. For example, such networks can be hacked into in the military, the usage of the system to attack friendly forces. A wireless Sensor network consists of thousands of low value, low energy and self-organizing nodes which are highly allotted. Due to the reason that the sensor nodes are highly distributed, there is a need of security in the network. Security is an important issue now these days in almost every network. There are few security issues and No. Of attacks that need to be look around and work upon. This paper discusses a number of the issues and the denial of provider attacks of security.

Keywords— ATTACKS, SECURITY ISSUES, , SECURITY REQUIREMENTS, WSN , WSN DEFENSES.

1. Introduction

Wireless Sensor Networks are heterogeneous systems containing many small devices referred to as sensor nodes and actuators with general-purpose computing factors. These networks will consist of hundreds or thousands of low value, low energy and self-organizing nodes which are highly allotted either in to the system or very close to it. These nodes include 3 principal components-sensing, data processing and conversation. Two other components are also known as aggregation and base station . Aggregation point's gathers data from their neighboring nodes integrates the collected data and then forwards it to the base station for another processing. Various programs of WSN includes habitat monitoring, production and logistics, environmental observation and forecast systems, military applications, health, business application and smart systems.

1.1. WSN Architecture

Field devices – Field devices are mounted inside the process and must be capable of routing packets on behalf of other devices. In most cases they manage the process or process devices. A router is a special kind of field device that does not have process sensor or control equipment and as such does not interface with the process itself.

Network manager – A Network Manager is responsible for configuration of the network, scheduling conversation between devices (i.e., configuring super frames), management of the routing tables and tracking and reporting the status of the network.

Security manager – The Security Manager is responsible for the generation, storage, and management of keys.

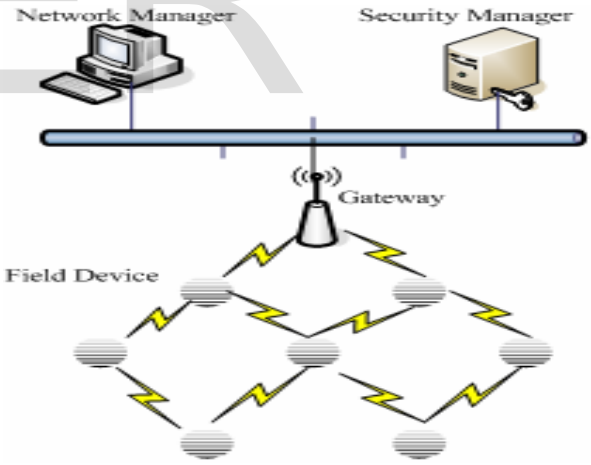


Fig.1: WSN Architecture

2. Security Issues

2.1 Limited Resources

All security techniques require a positive amount of resources for the implementation, including data memory, code space, and energy to power the sensor.

2.2 Limited Memory and Storage Space

A sensor is a tiny device with only a limited amount of memory and storage space for the code. In order to

construct an powerful security mechanism, it is necessary to restrict the code size of the security algorithm.

2.3 Conflicts

If the channel is reliable, the conversation may still be unreliable. The reason for that the broad cast natu re of the wire less se nso r network. If packets meet in the centre of transfer, conflicts will arise and the transfer itself will fail. In a crowded (high density) sensor network, this can be a main problem [4].

3. Security Requirements

Wireless Sensor network is prone to various attacks like any another conventional network, but its restricted resource characteristics and specific application features requires some extra security requirements including the standard network requirements. The goal of security offerings in WSNs is to protect the data and resources from attacks and misbehavior. The security requirements in WSNs consist of :

3.1 Authenticity and integrity

Most effective fact confidentiality is not enough to make sure the data security in WSN. As an adversary can exchange messages on communication or inject malicious message, authentication of records as well as sender also are crucial security requirements. Source authentication gives the truthfulness of originality of the sender. While records authentication ensures the receiver that the data has not been changed during the transmission.

3.2. Data Confidentiality

Data confidentiality is one of the critical security requirements for WSN because of its application purpose. Sensor nodes communicate sensitive data, so it is important to make sure that any intruder or other neighboring network could not get confidential information intercepting the transmissions. One of the security method of providing data confidentiality is to encrypt fact and use of shared key so that most effective receivers can get the sensitive information.

3.3 Availability

We cannot ignore the importance of availability of nodes when they are needed. For example, when WSN is used for tracking purpose in production system, unavailability of nodes may additionally fail to detect possible accidents. Availability ensures that sensor nodes are active in the network to meet the capabilities of the network. It should be ensured that security mechanisms imposed for data confidentiality and authentication are allowing the authorized nodes to participate within the processing of data or conversation while their services are needed. As sensor nodes have limited battery energy, useless computations can also exhaust them before their regular lifetime and lead them to unavailable sometimes; deployed security protocols or mechanisms in WSN are exploited by the adversaries to exhaust the sensor nodes by its resources and makes them unavailable for the network. So, security guidelines need to be implied so that sensor nodes do not longer do extra computation or do not try to allocate more resources for security reason.[11]

3.4 No repudiation

This denotes that a node cannot deny sending a message it has formerly sent. Non- repudiation is the warranty that someone cannot deny some thing. It refers to the capability to ensure that a node to a agreement or a communication cannot deny the authenticity of their signature on a message that they originated

3.5 Data Freshness

Data Freshness implies that the records is latest and ensures that no adversary can replay old messages. This prevents the adversaries from difficult the network by replaying the captured messages exchanged among sensor nodes. To attain freshness, security protocols need be designed in one of these way that they can identify duplicate packets and discard them preventing replay attack Moreover, as new sensors are deployed and old sensors fail, we suggest that forward and backward secrecy must also be taken in consideration.Any future messages after it go away the network.

4. OSI Layer wise threats and countermeasures

In this section, we discuss some of the known threats and countermeasures classifying in different OSI layers.[2]

Table 1 Physical Layer

Threat	Countermeasure
Interference	Channel hopping and Blacklisting
Jamming	Channel hopping and Blacklisting
Sybil	Physical Protection of devices
Tampering	Protection and Changing of key

Table 2 Data-link Layer

Threat	Countermeasure
Collision	CRC and Time

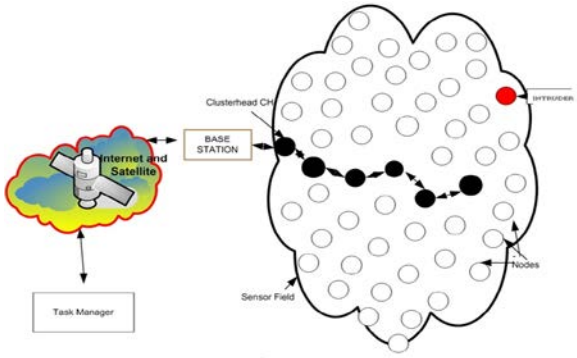
Exhaustion	Protection of Network ID and other information that is required to joining
Spoofing	Use different path for re-sending
Sybil	Regularly changing of
De-synchronization	Using different neighbors
Traffic analysis	Sending of dummy packet in
Eavesdropping	Key protects DLPDU from

Table 3 Network Layer

Threat	Countermeasure
Wormhole	Physical monitoring of Field devices and regular monitoring of Network using Source Routing. Monitoring system
Selective forwarding	Regular network monitoring using
DoS	Protection of network specific data Like Network ID etc.
Sybil	Resetting of devices and changing of
Traffic Analysis	Sending of dummy packet in quite hours; and regular
Eavesdroppig	Session keys protect NPDU From Eavesdroppers.

5. ATTACKS

Sensor networks are susceptible to numerous key styles of attacks. Attacks may be performed in a kind of approaches, most considerably as denial of service attacks, but additionally through traffic analysis, privacy violation, bodily attacks, and so on. A more effective node can easily jam a sensor node and effectively prevent the sensor community from performing its intended duty. We notice that attacks on wireless sensor networks are not specific to certainly denial of service attacks, but rather than encompass a spread of techniques together with node takeovers, attacks on the routing protocols, and attacks on a node's physical protection. In this section, we first deal with some common denial of service attacks and then describe additional attacking, consisting those on the routing protocols as well as an identity based totally attack referred as sybil attack.



5.1 Passive Attacks:

The tracking and listening of the conversation channel by unauthorized attackers are called as passive attack. The Attacks against privacy is passive in nature.

5.2 Active Attacks:

The unauthorized attackers monitors, listens to and modifies the data stream in the communication channel are called as active attack. Denial of Service attack eradicates a network's range to satisfy its expected function. Various DoS attacks on different layers are mentioned below:

A. Jamming

Jamming is one of the fundamental yet destructive attacks that strive to break in physical layer of the WSN structure.Jamming can be of two kind- constant jamming and intermittent jamming. Steady jamming influences the whole obstruct of the whole network whereas in intermittent jamming nodes are capable of speeaking records periodically however no logner continuously.

B. Physical Attacks

Physical attacks give the adversary the endowment to reconstruct the nodes and therefore the network functioning at physical layer. The attacker can summmry source code which ultimately provides attacker the information about the network that can alter the code to get admittance into the network. Attacker can substitute the nodes with the unlawful and detrimental ones, for negotiating the functioning of the whole sensor network.

C. Collision

Collision is a kind of link layer jamming that happens when nodes try to switch information at the identical time and on the same frequency [14]. An attacker may additionally reason collisions specially packets such as ACK manage messages. The effected packets are transmitted once more, growing the electricity and time value for transmission. Such an assault reduces the community perfection.

D. Exhaustion

Exhaustion happens at the link layer.This attack dominates

the engery resources of the nodes by causing them to retransmit the message even if there's no there is no collision or late collision [2].

E. Unfairness

MAC protocols at link layer administer the conversation networks by constraining priority schemes for seamless correlation. It is possible to use these protocols accordingly the precedence schemes, which ultimately results in decrease in service [2].

F. Neglect and Greed Attack

This attack occurs at the network layer [6]. When a packet is transmitted from a sender to a receiver, then in among each those nodes, there occur a number of other nodes through which the packet is routed before reaching to the final destination. Transmission is satated to achive success whlist the packet is absolutely reached to its destination. In the meantime, malicious node can force multi-hopping in the network, either with the splashing some packets or by routing the packets to a wrong node. This attack disturbs the behaviour of the adjoining nodes, which might not be able to receive or send messages.

G. Homing

In homing attack, the attacker investigates the network visitor at the network layer to interpret the geological area of cluster heads or base station adjoining nodes. It then implements some few attacks on those important nodes, so as to physically destroy them that further cause major destruction to the network [2].

H. Routing Information Alteration (spoofing)

It happensat the network layer [6]. In this, an adversary spots the routing data in the network via editing or replaying the routing information to disturb the traffic in the network. This attack can create new routing paths, attracts or repels the network vistor from decided nodes, lengthen or shorten the source routes, generates false error messages, causes network division and maximizes the end-to-end latency.

I.Black holes

Sink holes occurring at the network layer [12]. It construct a covenant node that seems to be very attractive in the sense that it promotes zero-cost routes to adjoining nodes with respect to the routing algorithm. This results maximum traffic to flow towards these fake nodes. Nodes adjoining to these harmful nodes collide for great bandwidth, thus resulting into resource contention and message destruction.

J. Flooding

Flooding also happens at the network layer [6]. An adversary constantly sends requests for connection establishment to the chosen node. To hit each request, some resources are allocated to the adversary by the way of targeted node. This can result into effusion of the memory and power resources of the node being bombarded.

K. Sybil Attack

This once more is a network layer attack. On this, an lousy node paffords more than one character in a network. It was originally described as an attack able to defeat the redundancy mechanisms of distributed data storage systems in peer-to-peer networks [10]. The Sybil attack is efficient enough to stroke different fault tolerant schemes such as dispersity, multi path routing, routing algorithms, data aggregation, voting, fair resource allocation, topology maintenance and misbehaviour detection.

L. Worm holes

In the wormhole attack, pair oflousy nodes first off discovers a wormhole at the network layer [12]. A wormhole is a low-latency junction between two sections of a network. The malicious node receives packets in one section of the network and sends them to another section of the network.

M. Hello Flood Attacks

Hello flood attack uses HELLO message to send itself to its adjoining nodes and a node receiving this message may consider that it is within radio vicinity of the sensor. In this type of attack, an adversary with a high radio transmission range and processing power sends HELLO message to a number of sensor nodes which are scattered in a large area within a WSN.

6. WSN Defences and Related Works

It is far very dificult to build up all of the protection necessities in a unmarried safety mechanism because the WSN has instense resource constraints and it has no predefined infrastructure. plenty of studies had been carried out and are on going to privilege the WSN with security support.WSN needs powerful, energy and resource efficient key control scheme for offering confidentiality, integrity and authentication security services. Link layer security mechanism in WSN can offer particular security support by using guaranteeing integrity, authenticity, and confidentiality of messages due to the fact they deny an outsider access to the network. Secure routing is another essential requirement for protecting WSN against external and insider attack. Right security answer for preventing DoS attacks at special layers is likewise a dire need for protecting the WSN from disruption.This segment discusses on cryptography and key establishment for WSN and then some security mechanisms regarding link layer and routing security of WSN are explored in some detail.

6.1 Cryptography

Cryptography is simple need for ensuring securityservices. Public key cryptography including Diffie-Hellman key agreement protocol or RSA signature is not suitable for WSN be- cause of its limitation in memory, computation and power. For example, to perform a single security operation RSA executes thousands or even millions of multiplication instructions. In wireless devices with few facilities, for

encryption and decryption RSA requires on the order of tens of seconds and up to minutes [4]. Whereas, symmetric cryptography and hash functions are faster and more computationally efficient than public key algorithms. That is why; most security schemes and security researches for WSN are based on symmetric key cryptography.

6.2Key Distribution / Management

One principle problem of symmetric cryptography is a way to distribute shared key to communicating nodes.Other problem is to preserve shared key secret only between the communicating hosts so that adversary's cannot get attain of it. That is why, besides light weight cipher, efficient key distribution and key management are fundamental security requirements for WSN. Self organization is an important aspect of WSN as the sensor nodes are deployed without following any pre established structure.In this case, WSN is divided into numberus of clusters, information is collected and processed by an aggregator node of each cluster and then transmitted to another aggregator forming a hierarchy and this data fusion saves energy of WSN. Here passive participation is another aspect, in which sensor nodes take actions based on messages from other nodes. In such instances, hierarchical key management is needed to provide security in different level of conversation in WSN. The following discussion is on some works based on these two kinds of key management protocol. [9]

6.2.1 **Key Pre-distribution Key Management**

Eschenauer and Gligor in introduced a random key predistribution scheme where the key distribution is divided into 3 phases which might be key pre-distribution, shared-key discovery, and path-key establishment. In key pre-distribution stage, a large pool of S keys and associated identifiers for each key are generated. That key pool a number of key earrings are generated byway of randomly drawing k keys along with their identifiers for each key ring after which every sensor node given a key ring. The base station stores the key rings of each node and the associated node identifiers. Also, each sensor node shares a pair wise key with the base station. In shared key discovery phase, after the deployment, each node broadcasts a list α, EK i (α) ; i= 1,. . ,k where α is a challenge.The nodes in the network can then delete the corresponding key from their key chain. This scheme is also known as basic scheme. In this key management scheme if the size of the network grows, each node in the network needs to store only a few keys, which is memory efficient and provides scalability. Again, when a node is compromised, the probability of an attacker to successfully attack a node is k/S where k«S.So, in key revocation process much communication overhead is not introduced as a small number of nodes are affected. But, this scheme is not able to provide node to node authentication which is a requirement to protect node replication attack (i.e., Sybil attack).

6.2.2 Hierarchical Key Management

Zhu et al.proposed Localized Encryption and Authentication Protocol (LEAP) for WSN which is a key management protocol. LEAP gives different security requirements for different kinds of messages exchanged among sensor nodes. For this cause, LEAP introduces four types of Keys for each sensor node which are individual key, pair wise shared key, group key and cluster key.

Each sensor node has a completely unique key named individual key which is shared with the base station to secure the messages among a sensor node and the base station.That key provides security when a node wants to share cluster key with its neighbor or a node sends data to the aggregator node.

Group key is shared among all the nodes in the network and the base station uses this key to provide security of broadcast message sent to the whole group.

Cluster key is a key shared by way of a node and all its neighbors. This key secures domesticaly broadcast message and supports in network processing and passive participation.The drawback of this scheme is that memory for every node to store 4 types of keys as well as computation and communication overhead increase if the density of WSN increases.

6.3 Link Layer Security

TinySec works at link layer and offer access control, message authencity, and integrity and message confidentiality. TinySec provides message security using cryptographic primitives- encryption and MAC. TinySec supports two of one kind security options: authenticated encryption (TinySec- AE) and authentication only (TinySec-Auth). In TinySec- AE, TinySec encrypts the data payload and authenticates the packet with a MAC. With TinySec-Auth, the packet authentication is performed with a MAC without encrypting the data payload.[3]

6.4 Secure Routing

In tradinoal networks the routing protocols in particully subject about the reliable delivery of messages. Message security (i.e. confidentiality, integration and authentication) and protection against DOS attacks are performed by end to end mechanisms such as SSL or SSH. As end to end conversation the main concern, there is no need for the midiator routers to know the content of the message except the necessary headers. But, the scenario is different in WSN where in many cases intermediate nodes need to communicate with each other for providing in network processing or data age gregation before sending the message to the base station. In this case, intermediate nodes have the ability to modify, sup-press or eavesdrop the message content and compromised node can exploit the features of routing protocol to cause potential damage of working functionality of the network. So, for WSN, routing protocols must be designed taking security also as a goal. For facilitating routing protocols with security mechanisms key management for each sensor node is an essential part which

has been discussed in the previous text. The following text is on some secure routing mechanisms for WSN. Proposed a routing protocol directed diffusion for WSN which is energy, bandwidth and memory efficient highly desirable for WSN. But this protocol is not able to afford secure group communication that is the conversation between sink and sources. Pietro et al. in extended this directed diffusion protocol to incorporate security in it.

7.Conclusion

With small sensor nodes, super low power consumption and alluring low value, Wireless Sensor Network is attracting uncountable application domains to experience and collect record. But, these attractive capability made Wireless Sensor Network difficult to combine security mechanism into it. This paper offers an idea of a main subset of security issues that Wireless Sensor Network faces due to its great design characteristics, communication and deployment pattern. At the same time, this paper includes short discussion on the crucial security aspects that are required to design a secure Wire Sensor Network. A few widely recognized attacks and their proposed counter measures are also discussed on this paper with the intention to provide an idea about how the Adversaries can actually attack the WSN exploiting its vulnerabilities and what sort of security awareness have to be taken into account when incorporating security mechanisms in WSN. In the end, this paper explores some works on three crucial security aspects of WSN which are key control, link layer security and secure routing. There are also many security elements of WSN together with secure data aggregation, intrusion detection, secure localization, etc. that are covered on this paper

Reference

[1] A. Banerjea, "A taxonomy of dispersity routing schemes for fault tolerant real-time channels," in Proceedings of ECMAST, vol. 26, May 1996, pp.129-148.

[2] Chris Karlof, David Wagner, "Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures", University of California at Berkeley.

[3] D.Boyle, T. Newe,"Securing Wireless Sensor Networks: Security Architectures", Journal of Networks, 2008, 3 (1).

[4] E. Shi and A. Perrig.Designing secure sensor networks. In *Wireless Communications, IEE*, volume 11, December 2004

[5] F. Anjum and P. Mouchtaris. *' Security for wireless Ad hoc networks Wiley* , 2007.

[6] J. Granjal, R. Silva, J. Silva, "Security in Wireless Sensor Networks", CISUC UC, 2008.

[7] J. Newsome, C. Mellon, and E. Shi. The sybil attack in sensor networks: Analysis and defenses. pages 259–268. ACM Press, 2004.

[8] J. R. Douceur, "The Sybil Attack," in 1st International Workshop on Peer-to-Peer Systems (IPTPS '02), March 2002.

[9] L. Eschenauer and V. D. Gligor. A key-management scheme for distributed sensor networks. In *CCS '02: Proceedings of the 9th ACM conference on Computer and communications security*, pages 41–47, New York, NY, USA, 2002. ACM Press.

[10]Mona Sharifnejad, Mohsen Shari, Mansoureh Ghiasabadi and Sareh Beheshti, A Survey on Wireless Sensor Networks Security, SETIT 2007.

[11] S. Datema. A Case Study of Wireless Sensor Network Attacks. Master's thesis, Delft University of Technology, September 2005.

[12] X. Du, H. Chen, "Security in Wireless Sensor Networks", IEEE Wireless Communications,2008.

[13] Y. Zou, K. Chakrabarty, "Sensor deployment and target localization based on virtual forces", INFOCOM 2003. Twenty-Second Annual Joint Conference of the IEEE Computer and Communications Societies. IEEE, Volume: 2, Pages: 1293 - 1303, April 2003.

[14] Z. Tanveer and Z. Albert. Security issues in wireless sensor networks. In *ICSNC '06: Proceedings of the International Conference on Systems and Networks Communication*, page 40, Washington, DC, USA, 2006. IEEE Computer Society.