A Survey on Various Attacks and Countermeasures in Wireless Sensor Networks

G. Santhi, PhD
Assistant Professor
Dept. of Information Technology
Pondicherry Engineering College,
Puducherry

R. Sowmiya
Student of M.Tech (IT)
Dept. of Information Technology
Pondicherry Engineering College,
Puducherry

ABSTRACT
For past few years, more interest has been focused on Wireless Sensor Networks (WSN) due to its wide range of applications in various fields. The WSNs are mainly used for sensing the pollution, monitoring the traffic; secure homeland, hospitals, military etc. There are possibilities of attacks in Wireless Sensor networks. Due to these attacks, there is possibility of loss of information. To avoid the data loss and for secure transmission of data, several countermeasures have been introduced. The main focus of this paper is to provide a detailed survey on various attacks and the countermeasures employed to safeguard the network from malicious attacks.

Keywords
Wireless Sensor Networks, Network attacks, Security challenges, Secure routing protocols

1. INTRODUCTION
A tiny device called nodes form the basic unit of Wireless Sensor Networks (WSN). These nodes are low cost tiny devices which are used in hundreds of thousands in number in WSN [1]. A node is also called as smart dust and sometimes as motes. A node comprises a processor, memory, battery, A/D convertor for connecting to a sensor. A device that senses the information and sends the information to a node is called Sensor. Sensors can sense the variations of physical environment such as Blood pressure, pulse rate, and stress. These Sensors mounted on a node can be of various types based on their purpose for which it is used. A sensor and a node together form a Sensor Node. The Nodes can be placed in a preferred particular position or by a random positioning in an area of deployment. These nodes can be moving from place to place in an area of deployment or fixed (static) in a place. Static nodes are commonly used in Networks. Wireless sensor Networks have one or more base stations which are having more resources and capability than nodes.

The main characteristics of a WSN include power consumption constrains for energy harvesting, cope with node failures, Mobility of nodes, Communication failures, Heterogeneity of nodes , Ease of use, Scalability to large scale of deployment. The security issues in WSN include the eavesdropping on the communication, lack of integrity, message replay attack, failure of authentication. Due to this attack, the false information is sent to the legitimate user.

2. SECURITY GOALS AND CHALLENGES
The security goals for reliable communication in WSN [2] are

- Data confidentiality

It is the most important issue in network security, messages should be hidden from a passive attack. As highly sensitive data are being communicated between sensor nodes, it is extremely important to build a secure channel in WSN.

- Data integrity

It is important to protect the messages that are being tampered or altered in WSN. An adversary is not just limited to modify the data that also can change the whole packet by injecting an additional packet.

- Data authentication

In WSN, it is always good to ensure that the data received is from the correct source. Always data received from destination node must be same as that sent by the source node.

- Data availability

It is vital to keep the data available for proper functioning of the network. User should be able to use the resources whenever they wish.

- Data freshness

The information received should be current and up-to-date. It should be ensured that there is no replay of any old content. It is important for security protocol to detect and discard the duplicate messages.

The security challenges of WSN are

- Energy constraint
- Network lifetime
- Topological changes
- Hostile environment
- Security issues
- Memory constraint

3. ATTACKS IN WIRELESS SENSOR NETWORKS
In Wireless Sensor Networks, nodes are usually deployed in an open unattended environment and hence they are prone for more physical attacks as they are not physically protected in that dangerous environment where they have been deployed [3]. The broadcast nature of the transmission medium makes the WSN more vulnerable to security attacks. As described in fig.1, attacks on WSN can be classified as Active attacks and Passive attacks.

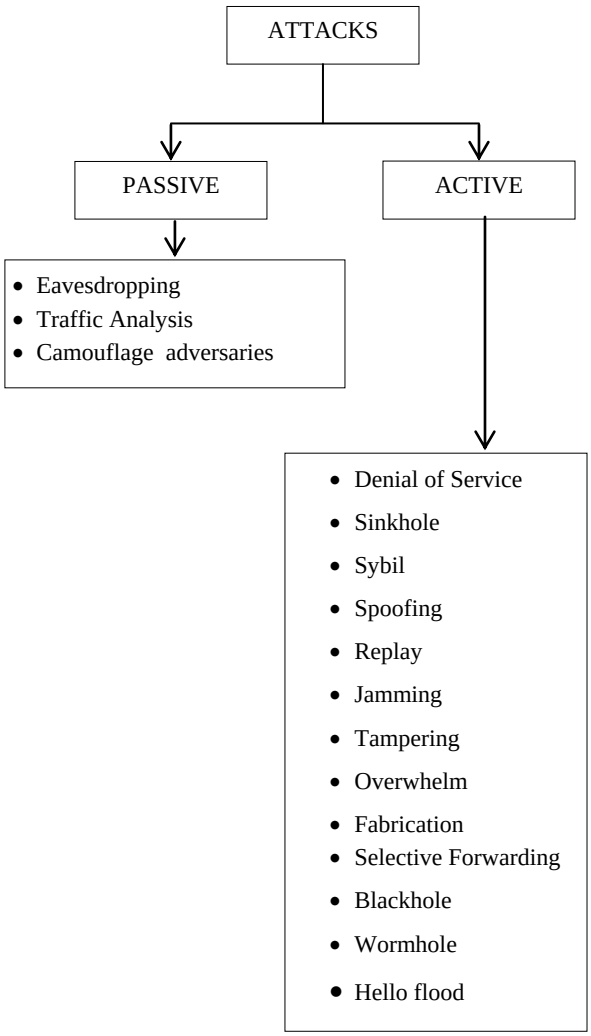

Fig: 1 . Classification of attacks in WSN

3.1 Passive Attacks

The monitoring and listening of the communication channel by unauthorized attackers are known as passive attack [4]. These attacks are mainly against data confidentiality. An unsecure traffic is observed and looked for clear text passwords and sensitive information, which are being captured by a passive attack and these information can be used in other types of attacks. The information on the network is not modified or changed in this attack. Decrypting weakly encrypted traffic, monitoring of unprotected communications, capturing authentication information and traffic analysis are passive attacks. Hence without the knowledge of the user there occurs a disclosure of information or data files to an attacker.

Some of the more common attacks against sensor privacy are:

3.1.1 Monitor and Eavesdropping

As the name implies it is an attack against confidentiality, a communication between two or more parties is monitored by an attacker to get possession of the transmitted data. This monitoring most commonly happens or done easily in a wireless network as the messages transmitted onto over the links are without any physical control. A passive attack, eavesdropping can be avoided easily by encrypting the data that has to be transmitted. But encryption cannot provide security to the data when attacks occur together with other attack, such as Cryptanalysis. This is the most common attack to privacy. The contents of the communication can be easily found by the adversary by snooping the data.

3.1.2 Traffic Analysis

Though data or messages transmitted with encryption for security, there is high chance of analysis of the communication patterns. Acquiring the knowledge about sensor activities an adversary can grasp sufficient information to cause malicious harm to the sensor network. Due to strong encryptions attackers cannot find the data as such but will get some clues about the data.

3.1.3 Camouflage Adversaries

In this a sensor node in a wireless sensor network is compromised by an adversary or attacker. This compromised node which is also called as camouflage node of WSN is used to masquerade the rest of the normal sensor node in WSN. The camouflage node then makes a false advertisement about the routing information in such a way that the further forwarding of packets from other nodes through the compromised node. Once the packets are received they are forwarded to a strategic node where privacy analyses of packet are done systematically.

3.2 Active Attacks

In active attack, an unauthorized attacker monitors, listen to and modifies the data stream in the communication channel. Here the attackers are no longer passive. Active measures are taken to achieve control over the network. This can be done by stealth, viruses, worms or Trojan horses. Some examples of active attacks are DoS, modification of data, black hole, replay, sinkhole, spoofing, flooding, jamming, overwhelm, wormhole, fabrication, Hello flood, node subversion, lack of cooperation, modification, man-in-middle attack, selective forwarding and false node.

3.2.1 Selective Forwarding

In this attack only certain packets are selectively dropped by a malicious node. Usually messages received are faithfully forwarded by nodes in sensor networks. The message or information received and sent should be same for a reliable and secure communication. When some compromised node refuses to forward and this result in loss of important data. In some cases all the packets are dropped and nothing is forwarded, called blackhole attack.

3.2.2 Blackhole Attack

The main aim of this attack is to lure traffic to a malicious part of the network. The compromised node of the sensor network attracts and fools the neighbor node by false advertisement. All the data from the fooled neighbor are forwarded to the lying node, instead of the destined base station. The specialized communication pattern and multi hop nature of the sensor network make it susceptible to this attack.

3.2.3 Wormhole Attack

The received messages are tunneled from one part of the network to another part of the network by an adversary [6]. In this attack, the tunnel is formed between one or more malicious node. The distant nodes are made to appear as close neighbor and so the energy resources of this node are exhausted quickly. This attack becomes effective when coupled with selective forwarding and Sybil attack, where it is very difficult to detect.

3.2.4 Hello Flood Attack

Hello Flood attack depends on the neighbor information to create routing path [7]. Every node in the network is made to

receive a powerful overhead packet broadcasted by an adversary announce themselves to the neighbors within a specific radio range. As long as it is within the same range the receiver node assumes the packet is uncompromised. Hello flood attack is an injurious active attack.

3.2.5 Denial Of Service

Denial of Service (DoS) is produced by the unintentional failure of nodes or malicious action [8]. It is the typical attack against availability. In this attack the nodes are kept busy by retransmission of legitimate request from other users or inserting new messages in the network. Hence the node is occupied and made unavailable leading to very slow performance.

3.2.6 Sinkhole Attacks

The sinkhole attack affects the Network layer. By using attractive bandwidth or path the attackers attracts the nearby motes. Therefore, the surrounding nodes are bogus done by the adversaries. It misroutes the information and it leads to packet dropping. This attack may further leads to selective forwarding attack or blackhole attack.

3.2.7 Sybil Attack

The attacker fools the neighbor nodes by having multiple identities [9]. By hacking the identities of the neighbor nodes, the attackers access the information of that correspondent node. The Sybil attack mainly focused on fault tolerant schemes such as dispersity, topology maintenance and multipath routing. As the adversary occurs in multiple locations, it confuses the geographic routing protocols.

3.2.8 Spoofed, Altered or Replay Attack

This is the most common attack in which the attack**e**r mainly focuses on the routing information. By spoofing, altering and replaying the routing information, the network topology gets confused and it leads to the packet loss. An attacker archives the traffic pattern without knowing the details about that, and it replays that information later to misinform the base station.

3.2.9 Jamming

An attacker attacks the topology by means of the radio frequencies of the network nodes [10]. The attack is more effective even in the single transmission of frequency. The adversary causes unnecessary energy depletion by adding the malicious packets in the topology. The network traffic is jammed and so the energy is dropped for the nodes. The nodes should follow some procedures to switch to sleep mode during jamming.

3.2.10 Tampering

The tampering attack affects the physical layer. The tampering replaces the entire node and gain access to sensitive information. The adversary extracts the cryptographic keys, so it results in loss of information. By this attack the node gets damaged physically.

3.3 Layer Oriented Attacks

WSN has a layered architecture. This WSN are more vulnerable for various kinds of attacks due to its layered architecture as shown in table.1. The physical layer attacks ranging from node capture to jamming of radio channel [11]. The data link layer coordinates the neighboring nodes to access shared wireless channel.

Table 1. Layerwise Attacks

NETWORK	ATTACKS
Physical Layer	• Jamming • Tampering
Data link Layer	• Collision • Exhaustion • Unfairness
Network Layer	• Spoofed • Replay • Selective forwarding • Sinkhole • Sybil • Wormhole • Hello flood
Transport Layer	• Flooding • Desynchronization
Application Layer	• Overwhelm • Repudiation • Data corruption

Collision, exhaustion and unfairness are the attacks in data link layer [12]. The network layer is vulnerable to various type of attack such as spoofed, sinkhole, wormhole and hello flood attack. In transport layer attack, there occurs the repeated request of new connections making the resource exhausted. Flooding and desynchronization are the attacks in the transport layer. Attacks such as overwhelm, repudiation, data corruption and malicious code are the different types of attack in application layer.

4. COUNTERMEASURES AGAINST THE ATTACKS

The main challenge in WSNs is to provide efficient security scheme by means of size of the sensor, memory, processing power and communication capacity [13]. For secure transmission over sensor networks, various cryptographic techniques are used. In order to avoid the attacks that tries to compromise a node and getting access to the entire network, various countermeasures and secure routing protocols [14] are given in table.2.

Table 2: Countermeasures and Secure routing protocols for various attacks

Attacks	Effects of attack	Countermeasures against Attack	Secure routing Protocols used
Jamming	• Confusion • Resource exhaustion Packets collision	• Spread Spectrum technique for radio communication • Use algorithms that take Radio Signal Strength Indicator (RSSI) values, carrier sense time and packet delivery ratio (PDR) techniques.	• LEACH
Tampering	• Hardware damage • Can gain access to higher level by extracting sensitive information	Using tamper-proof packing	• Direct Diffusion • SPIN
Collision	• Energy exhaustion • Interference • Discards packet	Error correction codes can be used	• LEACH
Selective Forwarding	• Packet dropping • Information loss	Transmit data through multiple paths	• Multipath Routing protocol
Sinkhole Attack	• Alter information • Drops packet • Resource exhaustion • Trigger blockhole, wormhole • Spoofing • Replay old message	• Key management • Authentication • Geographic routing	• PRSA • Geographical routing protocol
Sybil Attack	Threat to geographical routing protocols	• Authentication and encryption can prevent outsider attack • Use of public key cryptography prevents insider attacks	• Merkle hash tree • SIGF
Wormhole Attack	• Change in network topology • Information alteration	• Authentication • Encryption	• Adhoc on Demand Distance Vector (AODV) • Dynamic Source Routing (DSR)
Hello flood Attack	Data congestion	To Authenticate two way link before acting on information	• SPIN

5. SECURE ROUTING PROTOCOLS

A key management protocol SPINs (Secure Protocol for Information via Negotiation) which relies on a trusted base station for key distribution is proposed. SPINs consists of two parts: SNEP (Secure Network Encryption Protocol) and µTESLA (micro Time Efficient Streaming Loss tolerant Authentication). Many security properties like semantic security, data authentication, replay protection, data freshness, and low communication overhead are offered in this protocol [15]. The Tampering and Hello flood attack is resisted by means of SPIN protocol.

An authentication scheme Merkle tree has been proposed to avoid attacks [16]. Merkle tree found a wide application in cryptography due to its conceptual simplicity and applicability. It is a complete binary tree where the values of internal nodes are one way functions of the values of their children. It has various cryptographic applications such as certification broadcast authentication protocols, third-party data publishing, zero-knowledge sets and Merkle hash tree resist the Sybil attack.

6. CONCLUSION

The Wireless Sensor Networks are widely used in many applications. The need for security becomes the vital role. The secure communication is affected by means of various attacks. The network lifetime is reduced due to the energy drain of the nodes. To maintain data integrity and authenticity, steps are to be taken to resist active and passive attacks. The cryptographic techniques and the protocols are to be made stronger to avoid the attacks. Therefore, to maintain the secure network topology, stronger defensive techniques are used.

7. REFERENCES

[1] Daniel E. Burgner , Luay A, "Wahsheh "Security of Wireless Sensor Networks", Eighth International Conference on Information Technology: New Generations, 2011.

[2] Abhishek Jain, Kamal Kant and M. R. Tripathy, "Security Solutions for Wireless Sensor Networks", Second International Conference on Advanced Computing & Communication Technologies, 2012.

[3] Kahina CHELLI, 2015, "Security Issues in Wireless Sensor Networks: Attacks and Countermeasures", Proceedings of the World Congress on Engineering 2015 Vol I WCE 2015, July 1 - 3, 2015, London, U.K.

[4] Dhulkar, Ruchita, Ajit Pokharkar, and Mrs Rohini Pise, "Survey on different attacks in Wireless Sensor Networks and their prevention system", 2015.

[5] David Martins, and Herve Guyennet, "Wireless Sensor Network Attacks and Security Mechanisms: A Short Survey", IEEE, 2010.

[6] Hu YC, Perrig A, Johnson DV," Wormhole attacks in Wireless Networks", IEEE journal on selected areas in communications, 370-380, 2006.

[7] Magotra, Shikha, and Kush Kumar," Detection of HELLO flood attack on LEACH protocol", IEEE International Advance Computing Conference (IACC), 2014.

[8] David R. Raymond and Scott F. Midkiff, "Denial-of-Service in Wireless Sensor Networks: Attacks and Defenses", IEEE Pervasive Computing, Vol. 7, No. 1, pp. 74-81, 2008.

[9] Newsome J, Shi E, Song D, Perrig A, "Sybil attacks in sensor networks: analyses and defences", Third International symposium on Information processing in sensor networks, 259-268, 2004.

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

[11] Wang X,Gu W. Schosek K, Chellapan S, Xuan D, "Sensor Network configuration under physical attacks", ICCNMC, lecture notes in computer science, Springer, vol.3619, 23-32, 2005.

[12] Mohammadi, Shahriar, and Hossein Jadidoleslamy, "A comparison of link layer attacks on wireless sensor networks", arXiv preprint arXiv:1103.5589, 2005.

[13] Yanli Yu, Keqiu Li, Wanlei Zhou, and Ping Li, "Trust mechanisms in wireless sensor networks: attack analysis and countermeasures," Journal of Network and Computer Applications, Elsevier, 2011.

[14] Karlof C, Wagner D, "Secure routing in Wireless Sensor Networks: Attacks and Countermeasures", Adhoc networks, 293-395, 2003.

[15] Perrig A, Szewczyk R, Tygar JD, Wen V, Culler DE, "SPINS: Security protocols for sensor networks, Wirless Networks", 521-534, 2002.

[16] Kavitha, C., "A survey on secured routing protocols for wireless sensor network", In 2012 Third International Conference on Computing, Communication and Networking Technologies (ICCCNT'12), pp. 1-8, 2012.