A Survey On Types Of Cyber Attacks In Wireless Sensor Networks

[1 2] Dr.Jayashree Agarkhed , [2] Prof.Bhimaraya Patil,
[1] Professor, [2] Assistant Professor,
[1]Department of Computer Science And Engineering ,
[1]Poojya Doddappa Appa college of Enigineering , Kalaburagi,India

Abstract : Wireless Sensor Network (WSN)is a large scale network consisting of thousands of miniaturized autonomous ,versatile light weighted devices .Wireless Sensor network have a large of attack types that threaten data flow.So it is very important to provide integrity,confidentiality and availability.This paper,presents some idea about the challenges and security goals in WSNs & also the different types of attacks in WSN.

IndexTerms **- Challenges,Security goals,Cyber attacks,Wireless Sensor Network.**

I. Introduction

Wireless Sensor network is a collection of large number of sensor nodes of small size that interact with the environment with the help of sensors.sensor network can be used for target tracking,environment monitoring system control & chemical or biological weapons long before they get close enough to cause harm[1].The wireless sensor node is equipped with a limited power source such as a battery or even a solar cell.Sensor node lifetime depends battery lifetime.Power management is a key issue in system design,node design & communication protocol development.Efficient enery-consious clustering & routing algorithm can potentially prolong the network lifetime[2].
WSNs contain many self powered Wireless Sensor nodes (WSn) spread throughout the sensor field to sense some environmental parameters. The distance between WSn generally is limited to few meters. A sink node or Base station (BS) is responsible for collecting the data from all the nodes in the network in either single or multiple-hop manner. The BS sends the data collected to the end users through a gateway node, either through the internet or through any other communication channel. WSNs depend on dense deployment and co-ordination of nodes to carry out their tasks.

The sensor devices in WSNs are battery powered. The power of a sensor node is spent on sensing the environment and then to communicate the sensed data to neighboring nodes. The major reason of power consumption in WSN is communication, hence a high performance routing technique plays an important role in WSN. Routing is a process of finding a path from a source node to the destination node upon request of a data transfer. Finding efficient routes to forward data in WSNs differs from conventional routing in wired networks in several ways: lack of infrastructure; wireless links are non-reliable; sensor nodes may fail any time; and since sensor nodes are battery powered routing protocols have to meet consider energy savings requirements.
Routing mechanisms in WSNs are broadly categorized based on network structure and protocol operation. In general, based on the structure routing protocols in WSNs can be flat-based routing, hierarchical-based routing, and location-based routing whereas protocols based on protocol operation are multipath routing, routing based on queries, Quality of Service (QoS) routing and negotiation routing.
Some of the issues in routing in WSNs are:
1. Routing data in WSNs is bit challenging because of relatively huge density of WSn.
2. Most applications of sensor networks require the sensed data to flow from multiple sources to a particular BS.
3. Sensor nodes are tightly constrained in terms of energy, processing, and storage capacities. Thus, they require mechanisms for optimal resource management.
4. Sensor networks are application specific, i.e., design requirements and QoS requirements of a sensor network change with application.

This paper present a survey of WSNs vulnerabilities and security mechanisms. First, we present the WSNs specific constraints and their military applications. Then the security issues and attacks are outlined. Next, secure protocols are listed.

Threats to networks are numerous and potentially devastating. Up to the moment, researchers have developed Intrusion Detection Systems (IDS) capable of detecting attacks in several available environments. A boundlessness of methods for misuse detection as well as anomaly detection has been applied. Many of the technologies proposed are complement to each other, since for different kind of environments some approaches perform better than others. IDS do it by collecting data from network and analysis of transmitted packets inside the network. But generally IDSs do not act operative reaction against occurred attacks. IDSs usually have the state of informing administrator for occurrence of an intrusion.

Due to the nature of WSNs, attackers want to profit by constraints of WSN such as the hardware of sensor nodes and they try to make them non-serving by overloading them. Another attack approach is on physical layer. Attackers also want to achieve jamming and tampering attacks. In [9] as a countermeasure to jamming attack, it is described that the mapping protocol for nodes makes situational awareness in the neighboring nodes to notice a jamming attack using message diffusion. Addition to physical layer attacks, attackers can damage sensors and to avoid from this attack, users try to camouflage sensor in environment. Dos Attack Types on WSN Layers are described briefly.

II. WSN CYBER Attacks

There are two common types of security attacks, active attacks and passive attacks[3]. Passive attack is difficult to detect. Traffic monitoring, traffic analysis are some examples of passive attacks. In active attacks, an attacker tries to remove or modify the messages which are transmitted on the network.The examples of the active attacks includes jamming, message reply modification,DOS(Deniel of Service) [4] [5]. Based on these two attacks there are number of attacks and threats on the WSN to leak information ,slow down services by causing delayed response. Some of well known attacks includes:

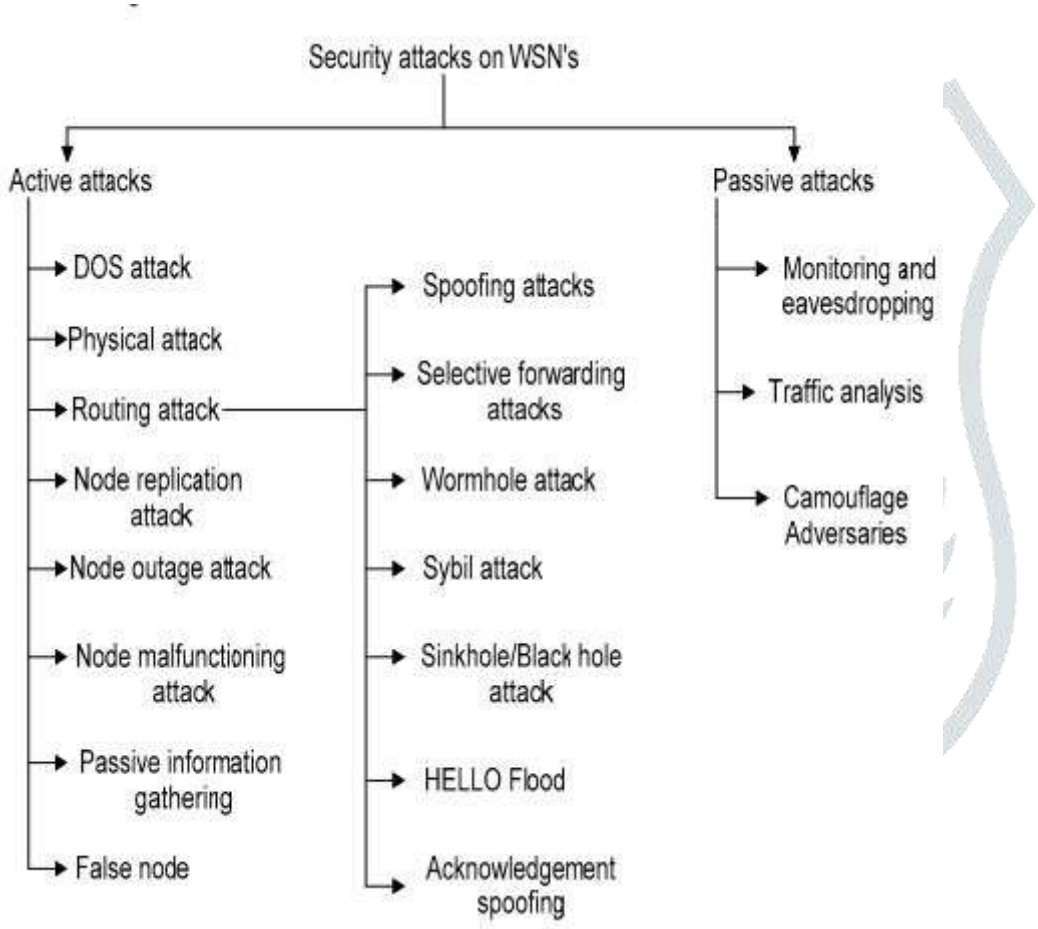

Figure 1: Classification of security attacks

.

In this paper we are mainly concentrating on only routing attacks which are explained below;

A. *Spoofing Attack:*

In this type of attack an attacker can change routing information between nodes, maximize delay from one of end of network to the other. An attacker can identify as another device or may creates multiple illegitimate identities.[6]

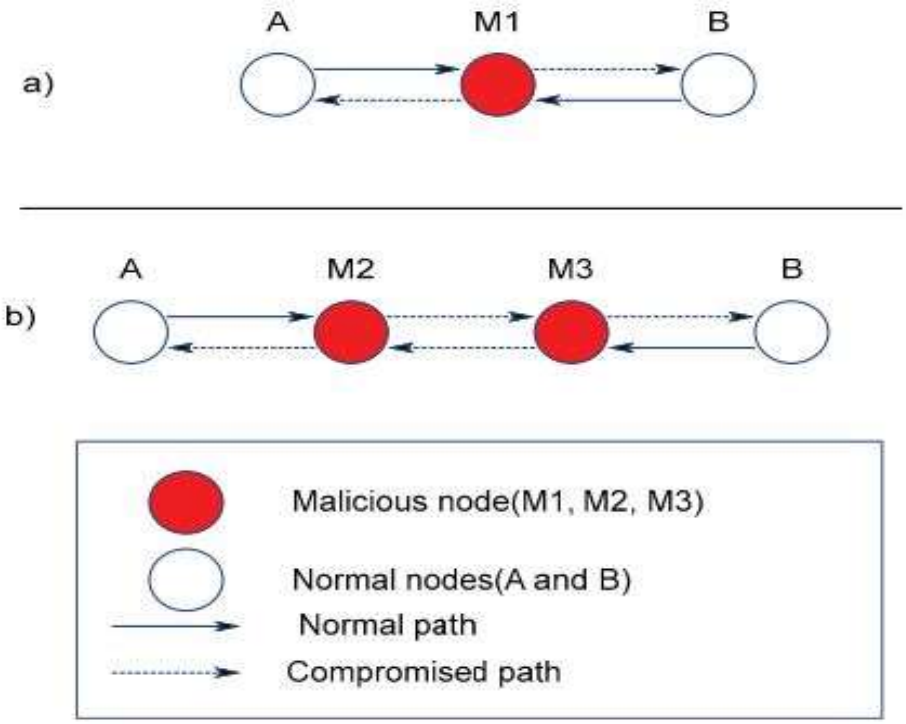

Figure 2: Spoofing attack

B. *Selective Forwarding attacks:*

In this type of attack,a malicious node select acct like normal node & forward packets but selectively drops some packets[7].

C. *Sinkhole/Black hole attacks:*

In this type of attack,attackers main goal is to attack the traffic from the nodes of particular region through a particular node called a black hole node by broadcasting the message that this is the only optimal route[8].

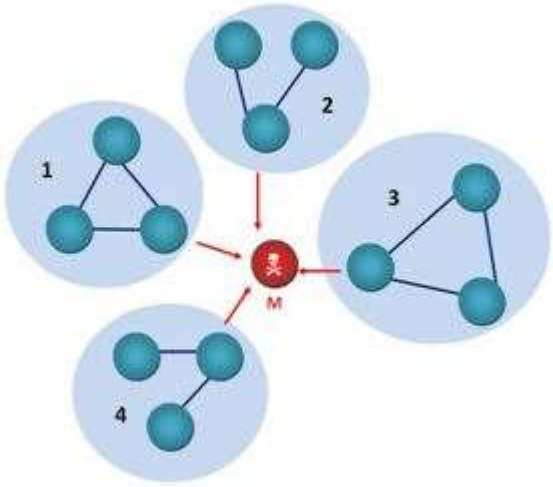

Figure 3: Sink/Black hole attack

D. *Sybil attack:*

In Sybil attack,a malicious node takes multiple identities.With this attack a malicious node can target the routing protocol ,leading to a corruption of the routing protocol,by creating a fake arbtitrary node[9].

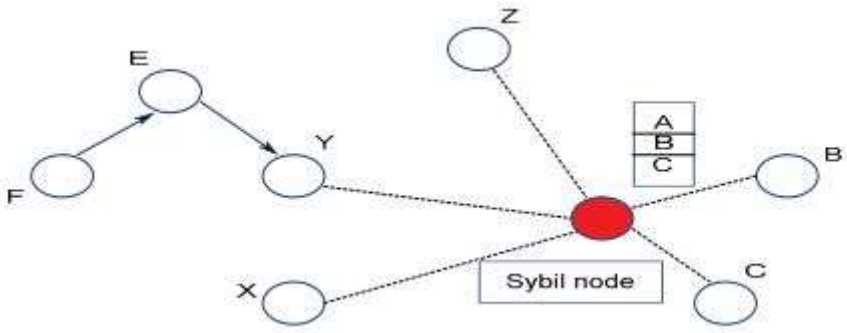

Figure 4:Sybil attack

E. Wormhole attack:

In this attack,an attacker records the message at one malicious node & tunnels them to another location.So this attack requies the insertion of two nodes to accomplish attack.These two malicious nodes are inteconnected .So these nodes achieve a distant location with a single jump & advertige as a shortest path to neighboring nodes & force them to use malicious nodes to route packets with this ,the information can be easily retrieved by the attacker[10].

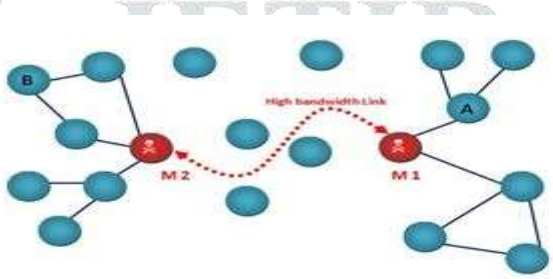

Figure 5:Wormhole attack

F. HELLO flood attack:

The routing protocol uses “HELLO packets” to find neighboring nodes.When a node receives such messages then it assumes that it is within radio range of sender.The attacker may use a high transmission power device & influence the every node in network that this is its neighbor[11].

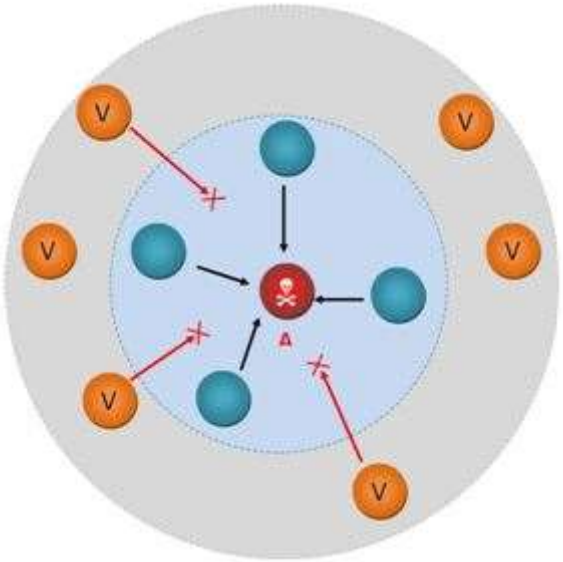

Figure 6 :Hello Flooding attack

G. Acknowledgment attack:

There are many protocols which are based on implicit or explicit link layer acknowledgments in WSNs. The attacker tells the other side that a dead node is still alive or that the link is strong enough.With this,an attacker capture packets sent to the dead node or the weak link ,spoof the acknowledgment & may influence the sending node that a weak link is strong & dead node is alive[12].

H. Deniel of Service attack:

In DoS attack,an attacker tries to make service or system unavailable .There are various DOS attacks including jamming attack & SYN flooding attack.In SYN flooding attack ,an attacker send large number of SYN packets to a victim node.The victim node send a SYN-ACK packet' & wait for ACK.The attacker will not send back the ACK.So the victim will not accept any other new connection unless pending connection get clear or buffer overflow occurs[13].

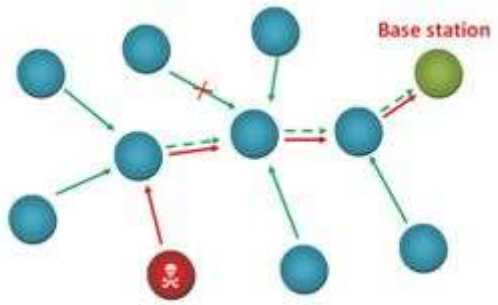

Figure 7: DoS attack

Comparison of attack types:

TYPE OF ATTACK	OSI LAYER	SECURITY MEASURES
Spoofing	Network layer	Encryption techniques
Selective forwarding	Network layer	Redundancy techniques, probing mechanism
Sybil attack	Network layer	Authentication mechanisms
Wormhole attack	Network layer	Authentication mechanisms
HELLO flood Attack	Network layer	2-way Authentication mechanisms,3-way Handshake
Acknowledegement spoofed	Network layer	Error Correction Code,ACK spoofed

III. WSN's SECURITY GOALS:

WSN's security contains all policies, mechanism and services that are required to protect the system against unauthorized access corruption of communication DOS. Generally any system must provide four main security goals which are confidentiality,integrity ,availability and authentication[14 [15] [16] [17].

a) Confidentiality: it is one of the security mechanism which ensures that the data should be accessible only to authorized users.
b) Authentication: it is another security mechanism which includes identity verification and validation. So its ability of receiver to check that the data is from the correct receivers.
c) Integrity: when a message is transmitted through a networks an unauthorized individual is not able to destroy or modify the information.
d) Availability: when an authorized user requests a data an interpretation should not accrue and it should be always available.

IV. CHALLENGES OF SECURITY IN WSN's:

WSN nodes have very limited energy memory and processing capabilities, the mail challenges faced by WSN's includes.

a) Energy constraints: the most important constraint in WSN is the energy sensor nodes possess limited energy and hence any processing overhead will affect their availability. So energy efficient algorithms can potentially prolong the network lifetime.
b) Remote location: WSN's development in remote and hostile environment makes them exposed to security breaches such as signal jamming, eavesdropping and spoofing.

c) Resource constraint: the available embedded memory in sensor node is very small and is shared by the operating system and processing unit.
d) Lack of central control: WSN is deployed with central point by control, due to their large scale and dynamic in nature,
e) Error prone communication: WSN's have no static topology and any node can join the network at any time. They possess wireless adhoc nature and other node can leave network voluntarily or being forced to quit network due to energy disruption. Topology control is also important is WSN's to preserve energy and network connectivity. So this may lead to failure of routers, collisions and packets may be lost or corrupted.

Conclusion And Future Work

In this paper,it is aimed to addrees cyber attacks occurring in WSNs,with a special focus on the security challenges & goals are described in details. In the future work,it is aimed to implement security approaches in a real WSN system.additionally a key management mechanism can be applied to WSN system to increase the security of the System[18].

REFERENCES

[1] JP Walters, Z Liang, W Shi, V Chaudhary Wireless sensor network secu-rity: A survey, Security in Distributed, Grid, and Pervasive Computing, Auerbach Publications, CRC Press, New York, USA, 2006.

[2] P. B. Hari, S. N. Singh, Security issues in Wireless Sensor Networks: Current research and challenges, International Conference on Advances in Computing, Communication, Automation (ICACCA) (Spring), Pages 1 - 6, September 2016.

[3] Sonal Garg, Vikas Malik, Review of Threats in Wireless Sensor Networks, International Journal of Emerging Technology and Advanced Engineering, Volume 6, Issue 9, September 2016.

[4] E. Y. Vasserman, N. Hopper, Vampire Attacks: Draining Life from Wireless Ad Hoc Sensor Networks, IEEE Transactions on Mobile Computing, Volume 12, no. 2, Pages 318 - 332, Feb. 2013.

[5] Naser Alajmi, Wireless Sensor Networks Attacks and Solutions, International Journal of Computer Science and Information Security, Volume 12, No. 7, July 2014

[6] iang Tang, Qiao Liang Li, S-SPIN: A provably secure routing protocol for wireless sensor networks, International Conference on Communication Software and Networks, 2009.

[7] C. Karloff, N. Sastry, and D. Wagner, TinySec: a link layer security architecture for wireless sensor networks, 2nd international conference on Embedded networked sensor systems, Baltimore, MD, USA, 2004.

[8] Leonard E. Lighfoot, Jian Ren, Tongtong Li, An Energy Efficient Link-Layer Security Protocol for Wireless Sensor Networks, IEEE EIT, 2017.

[9]K. CHELLI, Security Issues in Wireless Sensor Networks: Attacks and Countermeasures, Proceedings of the World Congress on Engineering, Volume 1, 2015.

[10]Ali K. Mubarak, Defenses against passive eavesdroppers in data peer-to-peer system, International Journal of Advanced Science and Engineering Research, Volume 1, Issue 1,Pages 834 - 841, June 2016.

[11]A. Mpitziopoulos, D. Gavalas, C. Konstantopoulos and G. Pantziou, A survey on jamming attacks and countermeasures in WSNs, IEEE

[12]. Jurdak, X. R. Wang, O. Obst, and P. Valencia, "Wireless sensor network anomalies: Diagnosis and detection strategies," in Intelligence-Based Systems Engineering. Springer, 2011, pp. 309–325.

[13] S. Rao, S. Deepak, and P. Pradeep, "Parametric analysis of impact of jamming in wireless sensor networks," in Wireless and Optical Commu-nications Networks (WOCN), 2013 Tenth International Conference on. IEEE, 2013, pp. 1–5.

[14] H. K. Kalita and A. Kar, "Wireless sensor network security analysis," International Journal of Next-Generation Networks (IJNGN), vol. 1, no. 1, pp. 1–10, 2009.

[15] S. Sharmila and G. Umamaheswari, "Detection of sybil attack in mobile wireless sensor networks," IJESAT] International Journal of Engineering Science & Advanced Technology, pp. 256–262, 2012.

[16]Q. Zhang, P. Wang, D. S. Reeves, and P. Ning, "Defending against sybil attacks in sensor networks," in Distributed Computing Systems Workshops, 2005. 25th IEEE International Conference on. IEEE, 2005, 185–191.

[17]C. Karlof and D. Wagner, "Secure routing in wireless sensor networks: Attacks and countermeasures," Ad hoc networks, vol. 1, no. 2, pp. 293– 315, 2003.

[18] V. P. Singh, S. Jain, and J. Singhai, "Hello flood attack and its countermeasures in wireless sensor networks," International journal of Computer Science issues, vol. 7, no. 11, pp. 23–27, 2010.