Comparison of Various Types of Attacks on Data Transfer in Wireless Sensor Network

Aditya Vishnoi, Ankit Saxena, Bharat Bhushan Agarwal

Abstract— *Today wireless sensors network is widely used in all the organization for their daily communication. A wireless sensors network is collection of nodes in a network. Every person performs all their daily transaction and communication with the help of internet. Today Wi-Fi is widely used everywhere as it needed no wire connection it always its work with the help of unguided media.*

The person always shares their information and data with the help of wireless transmission some time they share confidential information which needed more security. As in the network there is some unauthorized person who needed to access the personal and confidential information of information.

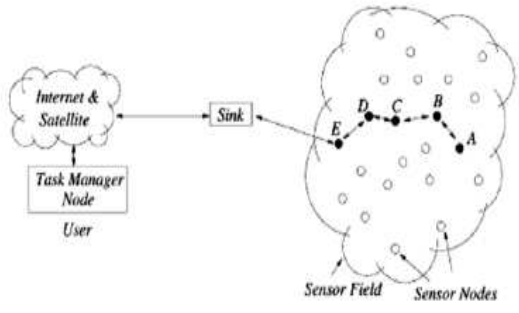
In this paper we compare all the types of attack which are done by the hacker over the wireless sensor network to access the information of another person. In this paper we define the causes and the method for this attack.

.

Keywords— Attacks on wireless sensor network, method of access information over wireless sensor network.

I. INTRODUCTION

This paper give the basic information regarding the wireless sensor networks its uses, components and the attack on it. The wireless sensor network is a self-configured and infrastructure less wireless networks for monitoring physical, likes Temperature, sound, vibration, motion or pollutants and to cooperatively pass their data through the network to a main location where the data can be used to observed and analysed. The following figure is providing the basic layout of the wireless sensor network.



A typical Wireless Sensor Network

II. WIRELESS SENSOR NETWORKS (WSN)

Today Wireless Sensor Networks has a wide range of applications in every field. They are more harmful to security attacks once deployed, as the nodes are unattended and unprotected in the network.

An adversary on the transmission path selectively drop packet is that in which the adversary same time transfer the packet and while in few occasions it drops the packet. It is very difficult to detect this type of attack since the packet loss may be due to unreliable wireless communication in the wireless sensor network.

In recent days, wireless sensor network are emerging as a promising and interesting area for communication. Wireless Network consists of a large number of heterogeneous /homogeneous nodes (usually called as nodes) which communicates through wireless medium and works cooperatively to monitor the environment. The total number of nodes in a network can vary from hundreds to thousands. Generally the nodes senses data from environment and send these data cooperatively to the sink/gateway node.

Mostly network is build only for a single application. Mostly WSN are used for applications such as military surveillance and disaster monitoring. Since its type of applications wireless sensor network is mostly deployed in hostile environment where it is unattended the architecture, each node consists of a radio transceiver for communication, micro controller for processing abilities, a for monitoring and battery for providing energy. Some of the popular applications of network are area monitoring and industrial and machine health monitoring ,environment monitoring, and waste water monitoring and military surveillance. The characteristics of nodes are

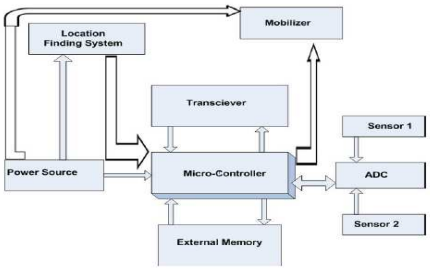
1. Resource Constraint
2. Unknown WSN topology before deployment
3. Unattended and unprotected once deployed
4. Unreliable wireless communication

Due to the above characteristics, wireless sensor network are easily vulnerable to attacks from hacker. Providing security solutions to these networks is difficult due to its

characteristics such as tiny in nature and constraints in resources.

III. COMPONENTS OF SENSOR NETWORK

Sensors can be scaled from micro sensors to larger scale .A sensor network consists sensor nodes which are small, lightweight and portable and these nodes form a network by communicating with each other directly or through other nodes. Some nodes among them will serve as sink(s) that are responsible of communicating with the user either directly or through the existing wired networks The main components of a sensor node as seen in the are microcontroller, external memory, transceiver, power source and one or more sensors. Every sensor node consists transducer, microcomputer, and transceiver and power source. The transducer (ADC—Analog to digital converter in fig 1) is responsible to generate electrical signals based on sensed phenomena and physical effects. The microcontroller's work is to process and store the sensor output. The transceiver receives command from a central computer or base station and transmits data to the computer or station. Sensor nodes are catered power by a battery. Some sensor nodes include external memory which may be on-chip memory of a microcontroller and Flash memory. Needs of memory of a sensor node are application specific. Each node may also belong to two extra components like: -Location finding system and Mobilizer. First one, location finding system is required since the user may in need of location with high accuracy and mobilizer may be needed to move sensor nodes to carry out the assigned tasks.

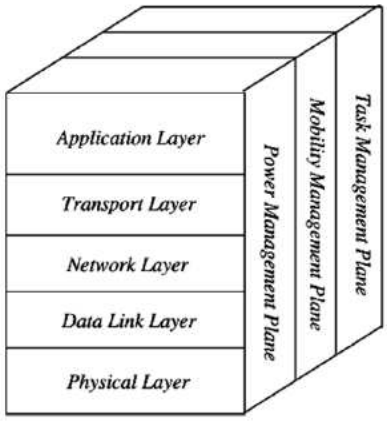


The components of a sensor node.

IV. COMMUNICATION STRUCTURE OF A WIRELESS SENSOR NETWORK

The sensor nodes are usually scattered in a sensor field as shown in Figure Each of these scattered sensor nodes has the capabilities to collect data and route data back to the sink and the end user. The data are routed back to the end user by a multi-hop infrastructure-less
Architecture through the sink. The sink may communicate with the task manager node via Internet or Satellite

.



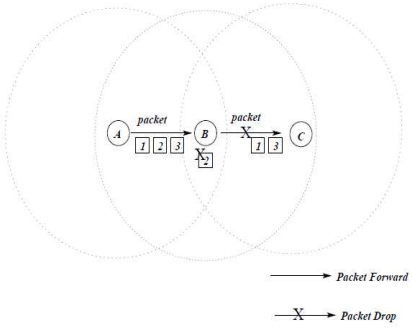
Wireless Sensor Network protocol stack

The protocol stack used by the sink and the sensor nodes is given. This type of protocol stack combines power and routing awareness integrates data with networking protocols communicates power efficiently through the wireless medium and promotes cooperative efforts of sensor nodes protocol stack consists of the application layer, network layer, transport layer data link layer, physical layer, power management plane, mobility management plane, and task management plane. This layer makes hardware and software of the lowest layer transparent to the end-user. The transport layer helps to maintain the flow of data if the sensor networks application requires it. The network layer takes care of routing the data supplied by the transport layer, specific multi-hop wireless routing protocols between sensor nodes and sink. The data link layer is responsible for multiplexing of data streams, frame detection, Media Access Control and error control. Since the environment is noisy and sensor nodes can be mobile, the MAC protocol must be power aware and able to minimize collision with neighbours' broadcast. The physical layer addresses the needs of a simple but robust modulation, frequency selection, data encryption, transmission and receiving techniques.

V. ATTACKS AND THEIR CLASSIFICATION

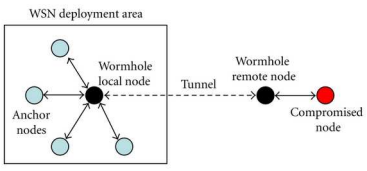
5.1 Selective Forwarding [2][3]

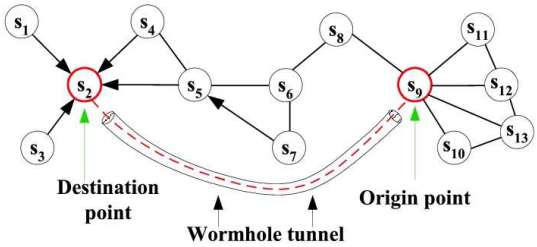
In the selective forwarding attack malicious nodes behaves like black hole and may refuse to forward certain messages and simply drop messages, ensuring that they are not propagated any further. However such an attacker runs the risks that neighboring nodes will conclude that she has failed and decide to seek another route. A more subtle form of this attack is when an adversary selectively forwards packets. The adversary interested in suppressing or modifying packets originating from a few selected nodes can reliably forward the remaining traffic and limit suspicion of her wrongdoing as shown in the following figure



5.2 Wormhole [1][4]

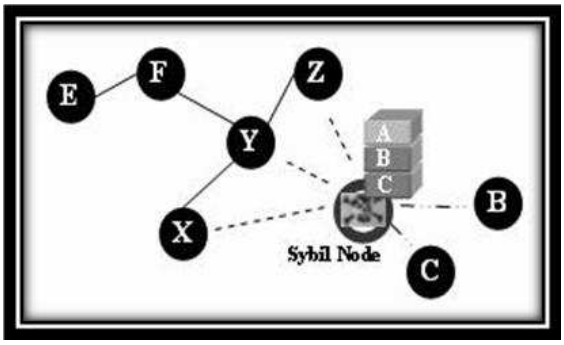
In the wormhole attack an adversary tunnels messages received in one part of the network over a low latency link and replays them in a another part. An adversary situated close to a base station may be able to completely disrupt routing by creating a well-placed wormhole. The adversary could convince nodes who would normally be multiple hops from a base station that they are only one or two hops away via the wormhole. The adversary on the other side of the wormhole can artificially provide a high-quality route to the base station, potentially all traffic in the surrounding area will be drawn through her if alternate routes are significantly less attractive.as shown in the following figure





5.3 Sybil

Sybil attack is a "malicious device illegitimately taking on multiple identities". In the Sybil attack, an adversary can "be in more than one place at once" as a single node presents multiple identities to other nodes in the network which can significantly reduce the effectiveness of fault tolerant schemes such as distributed storage and multi path. It may be extremely difficult for an adversary to launch such an attack in a network where every pair of neighboring nodes uses a unique key to initialize frequency hopping or spread spectrum communication. Sybil attacks also pose a significant threat to geographic routing protocols.



5.4 Acknowledgement Spoofing

Several network routing algorithms rely on implicit or explicit link layer acknowledgements. the inherent cause broadcast medium, in which an adversary can spoof link layer acknowledgments for "overheard" packets addressed to neighboring nodes. Goals include convincing the sender that a weak link is strong or that a dead or disabled node is alive.

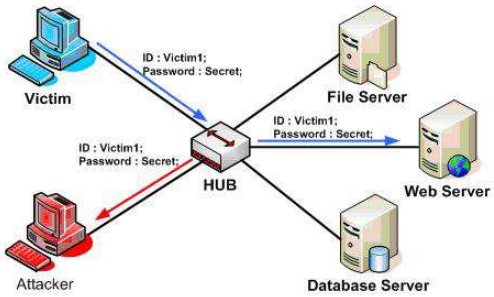
5.5 Impersonation

The node replication. This is also known as Multiple Identity, Impersonation [1][2]. Attacker seeks to add a node to an existing network by copying the node ID of an existing node. Node replication attacks can occur if an adversary can copy the node identification of a network node. In this manner packets could be corrupted, misrouted or deleted, and if this adversary could perform

this replication it is possible that cryptographic keys could be disclosed.

5.6 Eavesdropping

Monitor and eavesdropping. Also called confidentiality [4]. By listening to the data, the adversary could easily discover the communication contents. Network traffic is also susceptible to monitoring and eavesdropping. This should be no cause for concern given a robust security protocol, but monitoring could lead to attacks similar to those previously described. It could also lead to wormhole or black hole attacks.



5.7 Traffic Analysis

Traffic analysis attacks are forged where the base station is determinable by observation that the majority of packets are being routed to one particular nod[1][4]e. If an adversary can compromise the base station then it can render the network useless

VI. CONCLUSION

In this paper we have given the basic overview about the wireless sensor network . we have also define the components of sensor network. And we have also define the all the types of attacks done by hacker in the wireless sensor network to access the information of another person.

REFERENCES

[1] Hung-Min Sun, Chien-Ming Chen, and Ying-Chu Hsiao. Un-mask: Utilizing neighbor monitoring for attack mitigation in mul-tihop wireless networks. 2010

[2] Bo Yu and Bin Xiao. Detecting selective forwarding attacks in wireless networks. In *Parallel and Distributed Processing Symposium, 2006. IPDPS 2006.*

[3] Jeremy BroWSN and Xiaojiang Du. Detection of selective forwarding at- tacks inheterogeneous networks.Tran Hoang Hai and Eui nam Huh.

[4] Detecting selective forwarding attacks in wireless networks using two-hops neighbor knowledge.

[5] Tanveer Zia and Albert Y. Zomaya. Security issues in wireless networks.