Attacks that Decline the Proficiency of Wireless Networks

Amruth V[1], Mudassira Tahneet B. Lahori[2], Reema Abdul Rauf[2], Mariyamath Rifaina[2], and Jeril Kuriakose[3]
[1]Department of Information Science and Engineering, Bearys Institute of Technology, Mangalore, India
[2] Department of Computer Science and Engineering, Bearys Institute of Technology, Mangalore, India
[3] School of Computing and Information Technology (SCIT), Manipal University Jaipur, India

***Abstract*—Wireless Sensor Network (WSN) is an emerging technology, in any application wireless communications techniques happen to be an important tool. Since several users make use of this technique concurrently over one channel where security becomes a great concern. Although there are several methods to provide a safe network by protecting it from various attacks, but giving 100% security and sustaining confidentiality is a great challenge. This paper will give you a survey about the different attacks on a network such as Sybil attacks, Black hole attack, DOS attacks, Wormhole attack and Sinkhole attack.**

Keywords— Sinkhole attack; wormhole attack; security;sybil attack.

I. INTRODUCTION

The wireless sensor network consists of huge number of sensor nodes which are compactly arranged in a field of sensor. Without any wire connection every nodes are linked by infrared, radio frequency or other medium .This kind of network is called wireless sensor network. Consequently the progress of the networks, more than the years the network attack techniques and methods have greatly developed.

WSN are subjected to logical attacks as well as physical attacks. The Physical attacks concede node capture, and interfering with sensor nodes. Alternatively, logical attacks contains Sybil attack, Black hole attack, Wormhole attack, Sinkhole attack and the Distributed Denial of Service (DDoS) attack.

II. CATEGORIZATION OF WIRELESS ATTACKS

A. TYPES OF ATTACKS:

There are different types of network layer attacks in WSNs which can be mainly categorized as following:

- Passive attack
- Active attack

Passive Attack

The communication channel by unauthorized attackers is monitor and listens to are known as passive attack. It is classified as:

- Attacks against privacy are passive in nature

Active Attacks

The monitoring, listening and modifying the data stream of the communication channel by unauthorized attackers are known as active attack.

It is further classified as follows:

i. Routing Attacks which are active in nature. Its types are as follows:
   - Sybil Attack
   - Black hole Attack
   - Wormhole Attack
   - Sinkhole Attack
   - Selective Forwarding

ii. DOS Attack

iii. Other Attacks

a) SYBIL ATTACK

Sybil Attack in WSN: The name Sybil Attack is labeled after the topic in the book Sybil, a case study of a woman who has been diagnosed with various phony identities. These phony identities are identified as Sybil nodes [1]. Douccer introduced Sybil attack in peer to peer network [2]. The attacker can create various arbitrary identities or imitate other nodes identities in the network /MAC layer [3]. The various identities represented by a node to some other nodes in the network might be malicious node. The traffic move towards that particular malicious node and this reduces the effectiveness of error tolerant systems significantly, for instance disparity, multipath and distributed storage [4].

When there is no attack the normal energy utilized for network differ. In this, Sybil attack, it drains the entire energy at 100-150ms due to troubling of duplicate nodes in the path. In fig. 1 there is an energy loss from 200ms of simulation, more than 10% of energy is consumed when compared to normal operation [4].

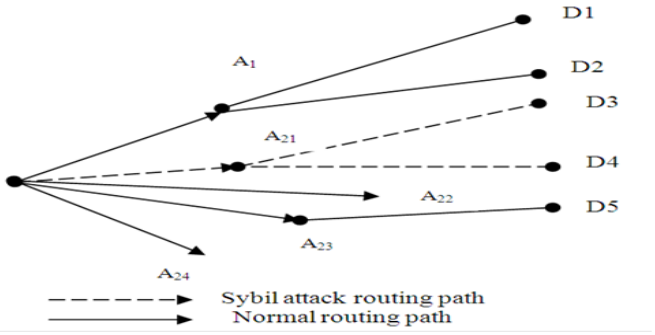

Fig1. Sybil attack.

b) BLACK HOLE ATTACK

A black hole is a nasty node that magnetize all the traffic in the network by doing publicity of containing the shortest path in the network So, it makes a figurative black hole with the nasty node or the opponent at the center, so the black hole drops all the packets it receives from the other nodes.

True control messages are not send in black hole. In order to carry out the attack, Nasty nodes wait for the adjacent nodes to send RREQ messages. When the nasty nodes get the RREQ message from its adjacent nodes, it straight away sends a false RREP message, providing a way to the destination over itself. In this way, it allocates a high series number to remain in the routing table of victim node before actual nodes sends an authentic reply. Therefore, requesting nodes thinks that the route discovery process is done and ignores RREP messages from further nodes and start transferring packets over nasty node. In this way, all the RREQ messages are attacked by the nasty nodes in the network. Thus, all the packets will be sent to the nasty node from where actually they are not at all forwarded and finally dropped. This is black hole akin [5].

The fuzzy logic algorithm will give the superior solution for reducing the data loss over the network [6].

BlackHoleDetect(S,D)

/* S is the source node and D represents the Destination Node over the network*/

{

1) The intermediate node will be searched during the start of the transmission and data will be sent to the identified nodes.

2) The intermediate node failed forwarding the probe message to the next node;

3) The communication rate is check using fuzzy logic on each Neighbor Node using the RESPONSE time for the intermediate node

If(FuzzyRule(Response Time)> HIGH)

{

The Attacker Node is Detected.

Update Neighbor Node Table & Routing Table for the Intermediate Nodes

}

4) The unresponsive node is incapable of responding to the probe message.

5) The diagnosis algorithm will then be called to decide which one is the case.

}

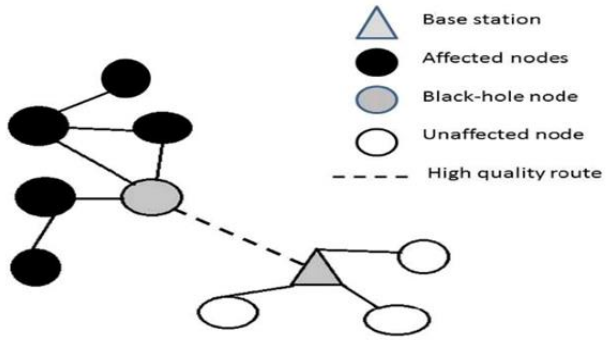

Fig. 3. Black hole attack.

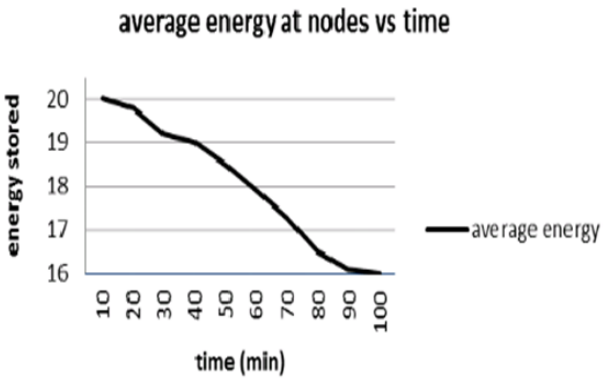

Fig. 4. Average energy at nodes vs time.

The Fig. 4 above shows the graph between the average energy of nodes and time, it also shows that the energy of nodes decreases with the increase in time [7].

c) WORMHOLE ATTACK

In attacks on wireless sensor networks, Wormhole attack is the severe network layer attack [8]. In this attack the opponent distract route from one section of network to a different section by using a wormhole link (tunnel) between two parts of the section [9].

Attackers will be able to develop a wormhole for packets which are not addressed to itself, owing to transmission of wireless networks. The signal processing techniques and hardware design, efforts have been done in order to protect against this attack. Another solution that we can have is to combine the various avoidance techniques into intrusion sensing systems [10]. Majority of present mechanisms of avoiding and examining the wormholes depend upon an exclusive hardware devices which consume a huge quantity of system resources otherwise, it does not meet the genuine hypothesis of combat zone application of WSN [11]. When there is no attack the normal energy utilized for network differs from 5-1 J. In wormhole attack energy drops to 0.5 J. From this values, it has been observed that power of the battery of sensor nodes was drained highly due to malicious nodes [13].

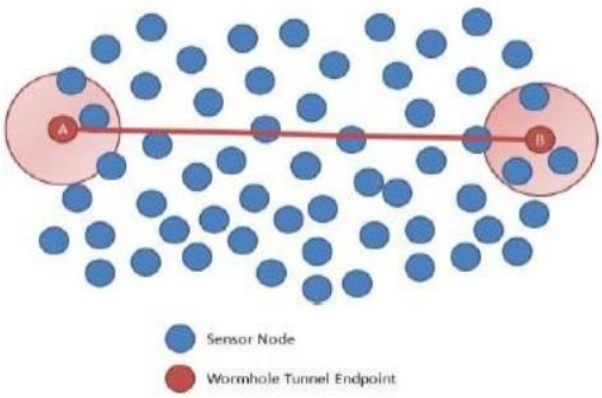

Fig. 5. Wormhole attack.

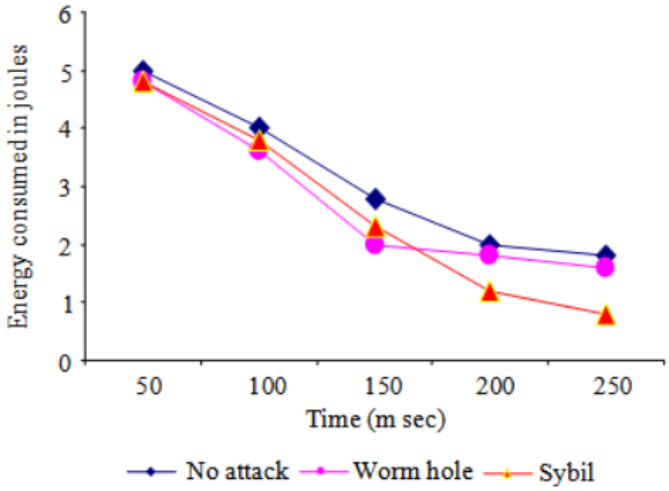

Fig. 6. Energy loss.

DOS ATTACK:

Denial of Service attack is a simple effort to make a network engaged for its legal users. An attacker interferes with data before it is actual read by sensor nodes, which results in false interpretations and finally leading to a wrong conclusion [14]. DoS attack allows an opponent to undermine, interrupt or raze a network and reduce a network's capacity to supply a service [15].

A DoS attack usually targets the physical layer applications in an environment where the sensor nodes are situated [1]. Layers of the protocol stack are extended by Dos attack. They are commonly very difficult to stop because they exist in several forms within the network. For instance, a nasty/ malicious node sends enormous number of requests to the main server which tests the validity of the nodes. Due to the enormous number of requests, the server becomes busy in examining all the illegal requests and hence it will not be obtainable for the actual legal users. This results in performance degradation of the whole network as the network gets packed due to the illegal requests [15].

Ordinary method of this attack includes saturating the targeted machine along with external communication requests so that it can't react to legal traffic, or responds gradually. Thus such attacks in turn lead to server overload [14]. A classic DoS attack structure is explained in Fig. 7.

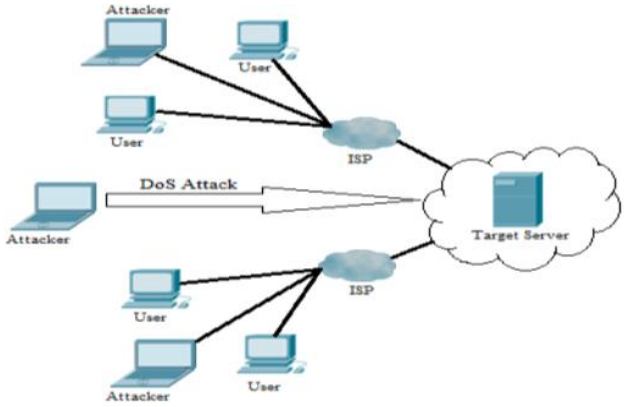

Fig. 7. Denial of service attack.

SINKHOLE ATTACK:

The Sinkhole attack in WSN is that an interloper uses a concession node in the sensor network of a specific region and attracts a number of or entire traffic of that specific region and creates a sinkhole. This attack is carried out by creating the conceded node which appear more appealing to all the adjacent nodes which contain an effectual routing track to the destination with high rate of energy.

When the attacker makes the sinkhole attack he will be able to make any kind of attack in WSN as all the traffic moves through that sinkhole node so that he will be able to assemble every data through the node and abuse the assembled data. [16]

Sinkhole attacks are not so easy to counter, since routing the information provided by the node is not easy to verify. For example, a laptop-class opponent has a radio transmitter of strong power that permits it to supply a high-quality path by transmitting with sufficient power to achieve a wide region of network [17].

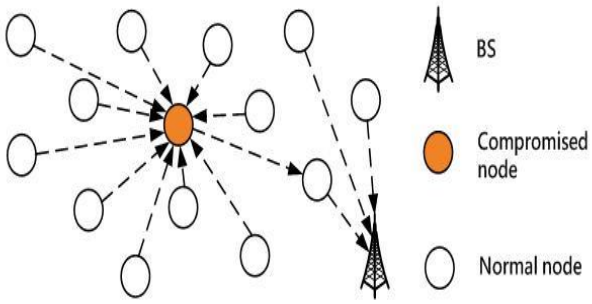

Fig. 8. Demonstration of a sinkhole attack.

III. PREVENTION OF WIRELESS ATTACKS

The following are the account by various researchers to identify and detect sinkhole attack in wireless sensor network. It can be categorized into following methods:

Anomaly-based: in this type of detection defines the normal behavior of user and the intrusion detection strategy is to search for anything that appears anomalous in the network.

Rule based: are planned based on the technique or behavior that is used to begin sinkhole attacks. These policies are fixed

in interruption detection scheme flowing on particular specialized monitors or sensor nodes.

Statistical: In this accost data that is associated with certain action of the nodes in network is noted.

Cryptographic: In this accost the authenticity and integrity of packets moving in the network is defended by using decryption and encryption keys.

Hybrid: In this accost is capable to hold any skeptical nodes when their signature is not integrated in identifying database [18].

IV. DISCUSSION

Comparing each attack Based on its packet loss and corrupted during transmission, a graph is plotted for each attack which is as follows: [19]

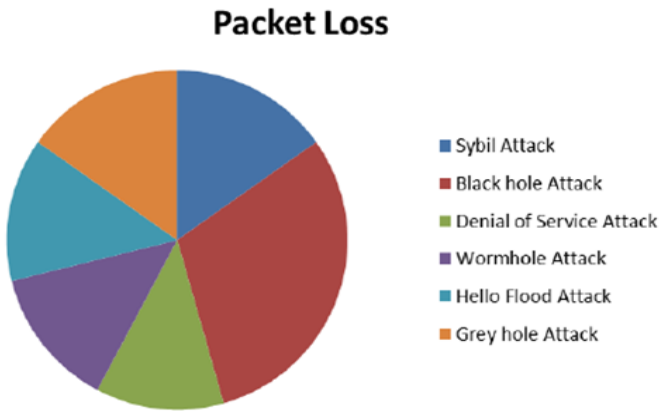

Fig. 9. Comparison of attacks based on packet loss.

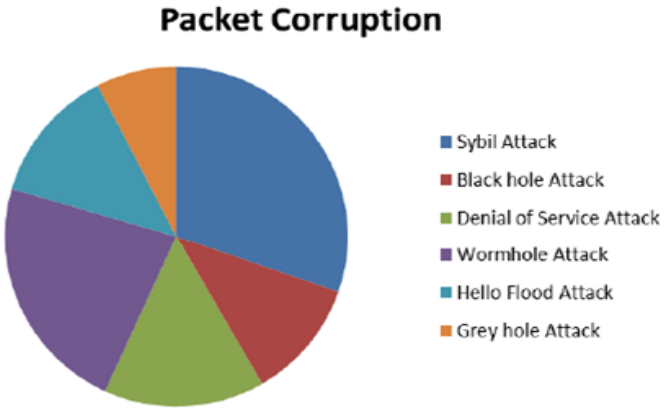

Fig. 10. Comparison of attacks based on packet corruption.

V. CONCLUSION

In this paper, we have discussed about various types of attacks on WSNs. Compared to conventional networks, Wireless sensor networks (WSN) are more susceptible to attacks. As the wireless communications are not consistent usually there will be loss of data packets due to attacks in WSN. Even though there are various attacks and the people shouldn't give up security system, but there is not a single solution to protect against every threat. Although, in this paper we have tried to present a brief study on the severity of attacks in WSN.

REFERENCES

[1] Karlof, Chris, and David Wagner. "Secure routing in wireless sensor networks: Attacks and countermeasures." *Ad hoc networks* 1.2 (2003): 293-315.

[2] Ma, Wei, et al. "Sybil-Resist: A New Protocol for Sybil Attack Defense in Social Network." *Applications and Techniques in Information Security*. Springer Berlin Heidelberg, 2014. 219-230.

[3] Deng, Jing, Richard Han, and Shivakant Mishra. "Countermeasures against traffic analysis attacks in wireless sensor networks." *Security and Privacy for Emerging Areas in Communications Networks, 2005. SecureComm 2005. First International Conference on*. IEEE, 2005.

[4] Kuriakose, Jeril, et al. "A Comparative Analysis of Mobile Localization and its Attacks." *Proceedings of the 2014 International Conference on Information and Communication Technology for Competitive Strategies*. ACM, 2014.

[5] Kong, Jiejun, Xiaoyan Hong, and Mario Gerla. "A new set of passive routing attacks in mobile ad hoc networks." *Military Communications Conference, 2003. MILCOM'03. 2003 IEEE*. Vol. 2. IEEE, 2003.

[6] Ahmed, Firoz, Seok Hoon Yoon, and Hoon Oh. "A bullet-proof verification using distributed watchdogs (BPV-DW) to detect black hole attack in mobile ad hoc networks." *Advances in Grid and Pervasive Computing*. Springer Berlin Heidelberg, 2012. 312-322.

[7] Prathapani, Anoosha, Lakshmi Santhanam, and Dharma P. Agrawal. "Detection of blackhole attack in a Wireless Mesh Network using intelligent honeypot agents." *The Journal of Supercomputing* 64.3 (2013): 777-804.

[8] Kuriakose, Cyril, et al. "Confiscation of Malicious Anchor Nodes in Wireless Sensor Networks." *Int. J. of Recent Trends in Engineering & Technology* 11 (2014).

[9] Ho, Jun-Won, Matthew Wright, and Sajal K. Das. "Distributed detection of mobile malicious node attacks in wireless sensor networks." *Ad Hoc Networks*10.3 (2012): 512-523.

[10] Edwards, J. J., J. David Brown, and P. C. Mason. "Using covert timing channels for attack detection in MANETs." *MILITARY COMMUNICATIONS CONFERENCE, 2012-MILCOM 2012*. IEEE, 2012.

[11] Zhou, Jie, et al. "Analysis and countermeasure for wormhole attacks in wireless mesh networks on a real testbed." *Advanced Information Networking and Applications (AINA), 2012 IEEE 26th International Conference on*. IEEE, 2012.

[12] Sadeghi, Mohammad, and Saadiah Yahya. "Analysis of Wormhole attack on MANETs using different MANET routing protocols." *Ubiquitous and Future Networks (ICUFN), 2012 Fourth International Conference on*. IEEE, 2012.

[13] Raju, R., et al. "A review on host vs. Network Mobility (NEMO) handoff techniques in heterogeneous network." *Reliability, Infocom Technologies and Optimization (ICRITO) (Trends and Future Directions), 2014 3rd International Conference on*. IEEE, 2014.

[14] Syed, Zeba, et al. "A novel approach to naval architecture using 1G VLAN with RSTP." *Wireless and Optical Communications Networks (WOCN), 2014 Eleventh International Conference on*. IEEE, 2014.

[15] Kuriakose, Jeril, et al. "A review on localization in wireless sensor networks."*Advances in signal processing and intelligent recognition systems*. Springer International Publishing, 2014. 599-610.

[16] Krontiris, Ioannis, et al. "Intrusion detection of sinkhole attacks in wireless sensor networks." *Algorithmic Aspects of Wireless Sensor Networks*. Springer Berlin Heidelberg, 2008. 150-161.

[17] Ngai, Edith CH, Jiangchuan Liu, and Michael R. Lyu. "An efficient intruder detection algorithm against sinkhole attacks in wireless sensor networks."*Computer Communications* 30.11 (2007): 2353-2364.

[18] Kuriakose, Jeril, et al. "A Review on Mobile Sensor Localization." *Security in Computing and Communications*. Springer Berlin Heidelberg, 2014. 30-44.

[19] Zhao, Ziming, et al. "Risk-aware mitigation for MANET routing attacks."*Dependable and Secure Computing, IEEE Transactions on* 9.2 (2012): 250-260.

[20] Felt, Adrienne Porter, et al. "A survey of mobile malware in the wild."*Proceedings of the 1st ACM workshop on Security and privacy in smartphones and mobile devices*. ACM, 2011.