International Journal of Scientific Research and Engineering Development-– Volume 3 Issue 6, Nov-Dec 2020

Available at www.ijsred.com

RESEARCH ARTICLE OPEN ACCESS

An Efficient Approach to Detect DoS Attacks in Wireless Ad hoc Sensor Network

Isaac Sajan R*, Jasper J**
*(Department of CSE, Ponjesly College of Engineering, and Nagercoil
Email: isaacsajan@gmail.com)
** (Department of EEE, Ponjesly College of Engineering, and Nagercoil
Email:mailtojasper@gmail.com)

----------**********----------

Abstract:

Wireless Sensor Network (WSN) comprises large number of sensor nodes, which is capable of transmitting information to a shorter distance in low bandwidth with low power consumption. Sensor nodes are deployed in an environment that cannot be reached easily which makes the network vulnerable to attacks. Vampire attack is one of such DoS attacks where attackers choose a longest path while transmitting data to sink. Vampire attack affects the throughput of the network and even leads to the failure of the network. So detection of such attacks and preventing it is necessary. Comparing to other forms of attacks, detecting vampire attack is difficult as the attacking node have all the necessary information of its network before attacking a node. We present in our paper a comprehensive survey on various types of DoS attacks in WSNs and approaches to prevent vampire attack using KID-LEACH. Simulation results shows KID-LEACH protocol performs better when compare to the existing protocols.

Keywords — **Vampire attack, Wireless Sensor Network, Security, Power Consumption**

----------**********----------

I. INTRODUCTION

Now a day's Wireless Sensor Networks (WSN) are popular in many areas such as military applications, smart houses, Tracking of Health etc. the nodes in this network senses the changes happening in any environment such as physical, mechanical environment and transmit it to the sink[10]. There are various limitations in WSN like processing power, memory resources and battery power. First method to reduce the energy cost is that the nodes that sense the changes should perform proper signal processing, aggregation and computation before transmitting the data to the base station. One of the important routing protocol that distributes power evenly to all the sensor nodes is the Low- Power Adaptive Clustering Hierarchy (LEACH) protocol [9]. This protocol is cluster based and all the nodes in the cluster should send the data only to the cluster head. The cluster head compress and aggregate the data and transmit it to the base station.

In Wireless Sensor Networks, the way of transmitting data between the nodes are wireless and therefore there is possibility for the nodes to be attacked by some malicious nodes. The effect of the attack will be more if the cluster head becomes the attacker. In such cases, there is a possibility for the whole data of the cluster to be affected by any attack in WSNs such as black Hole attack, Sybil attack, Worm Hole attack, Gray Hole attack, Flooding attack, etc. The routing protocols such as

LEACH, HEED, and PEGASIS do not provide any security measures to avoid those attacks [8,11].

In this paper, we will discuss how a malicious node exploits the LEACH protocol and yields vampire attack. To secure Wireless Sensor Network against Vampire attack, it is important to understand behavior of the attacks. We have done the analysis by using the NS2 simulator.

II. SECURITY GOALS IN WSN

Traditional network shares some common features of Wireless Sensor Networks [7]. The Security Goals of traditional network are as follows

A. **Data Confidentiality:** Limiting the access of secured information to the authorized user and preventing access by an unauthorized user. In any network data confidentiality is an important issue to be concentrated.

B. **Data Authentication:** Ability of a receiver to verify the data whether it received its data from a correct sender. The receiver must be able to identify if it has received the packets from the correct source. Data authentication can be achieved by cryptography where the data's can be encrypted and decrypted

C. **Data Availability:** Ability to determine whether the services are available during failure or during network attacks. Even a single point failure can affect the entire network so data availability is a prime issue.

D. **Data Integrity:** Ability to ensure that the information it received is not altered during transmission from the source to the destination.

III. CLASSIFICATIONS OF ATTACKS

The attacks are mainly categorized as passive attack and active attack. In a passive attack, the attacker snoops the transmitted data in the network but do not alter it. Hence the normal operation of a network is not affected. But in active attack, the attacker modifies, deletes and fabricates the data. Hence the normal operation of a network is totally disturbed[12]. The other category of attack is External attack and Internal attack. In an External attack, the attack is done by a node which does not belong to the network but in Internal attack, the attack is carried out by a node which belongs to the network and hence the detection of Internal attack is difficult, The traditional cryptographic methods do not suit the internal compromised nodes. Possible attacks on different layers are tabulated [5,6].

Table 1.Attacks on Different Layer

LAYERS	ATTACKS
Physical	Alteration, Eavesdropping, Jamming
Data Link	Flooding, Selfish MAC, Unfairness
Network	Vampire, Gray Hole, Black Hole, Sybil, Worm Hole
Transport	De-Synchronization, Syn-Flooding
Application	Buffer Overflow ,Logic Overflow

We focus on the attacks on the network layer in our research. The various routing attacks in network layer are as follows [3,4].

Table 2.Routing Attacks on WSN

Attack	Definition	Effects
Vampire	Uses protocol Compliant messages to drain resources.	Exhaust network resources, Route misdirection
Gray Hole	Selective dropping of packets	Packet loss and information fabrication, Suppresses messages in an area.
Eaves Dropping	Overhearing channel to get confidential data	Reduces data confidentiality, Threatens privacy protection.
Traffic Analysis	Monitoring network traffic and parameters that affect network	Increased packet collision &contention, Traffic distortion.
Camouflage	Malicious nodes masquerade as normal nodes to attract packets	Degradation of performance, Increase packet loss.
Sybil	Malicious nodes uses multiple fake identities to attract packets	Modifies routing information, False sensor reading
Black hole	Attracts traffic to a compromised node.	Exhausts network recourses, Modifies routing information
Hello Flood	Message transmission by malicious node with high transmission power to make other node believe as it neighbor.	Misleading routes generated, Confusion, Packet loss, Route disruption

Worm hole	Tunnelling messages from one location to another using low latency link	Forged routing, Changes network topology

All paragraphs must be indented. All paragraphs must be justified, i.e. both left-justified and right-justified.

IV. NEED FOR KID-LEACH PROTOCOL

We assume that the energy of the malicious node will be higher than the energy of the other normal nodes, so there is a high possibility of malicious node to become a cluster head. In this way the malicious node can become a cluster head and then can perform a vampire attack on the network by creating delay while forwarding packets[1].

In vampire attack, malicious node initially exploits the LEACH protocol to advertise it as a node that has high probability of becoming a cluster head.[2] There are different possible ways vampire exhibits its behavior. Malicious node can forward the packet in loop there by creating a delay in transmitting packet. Another type of vampire attack is that the malicious node may forward a packet to the farest node rather than the nearest neighbor thereby causing delay. vampire attack also shows random behavior by randomly causing delay of packets in its network. Hence detecting vampire attack is very difficult and there is a need for modification in the LEACH protocol.

Knowledge Intrusion Detection – LEACH evaluates the fitness of the node using the parameters like residual energy, delay and distance. If the evaluation value of the node is high the node is trustable and non-malicious. If the evaluation value is low then the node is malicious node.

V. KID-LEACH ALGORITHM

The algorithm for Vampire identification and removal of malicious node is as follows

Step 1: Path Discovery process
Step 2: Collecting information from all nodes
Step 3: Identification of nodes with highest evaluation value
Step 4: Confirmation of node as vampire node
Step 5: Removal of vampire node
Step 6: Broadcasting the information of the vampire
Step 7: Continue default routing process

VI. SIMULATION RESULT

Assumption made while simulation are: Base station have the highest energy, malicious node has more energy X times than normal node, sensor node are static and at every frame all nodes has data to transmit. Simulation using Matlab version 9 using normal desktop system results are based on the simulation of 500 sensor nodes. Malicious nodes are selected randomly; the network intensities are varied from 100,200,300,400,500. Analysis are done to determine its performance. Parameters used are vampire detection rate and Average delay analysis in the presence of vampire attack.

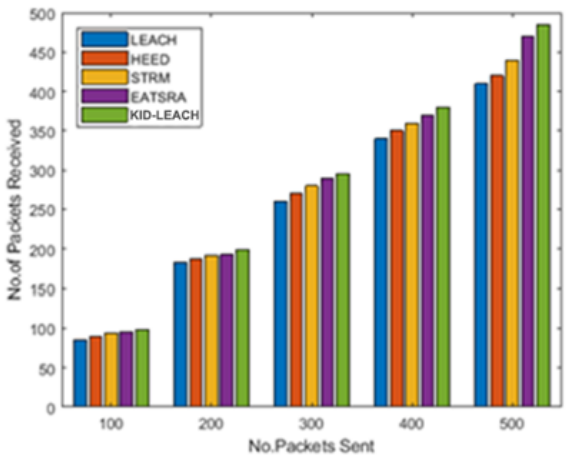

Figure 1.Vampire Detection Rate

The base station in the absence of vampire node receives good amount of packets. It is observed that the number of packets received at the sink reduces in the presence of malicious node, as the malicious node delay packets while forwarding data to the other nodes. When the no of nodes sent is about 500 the efficiency attained is about 94%, which is better than other existing protocols.

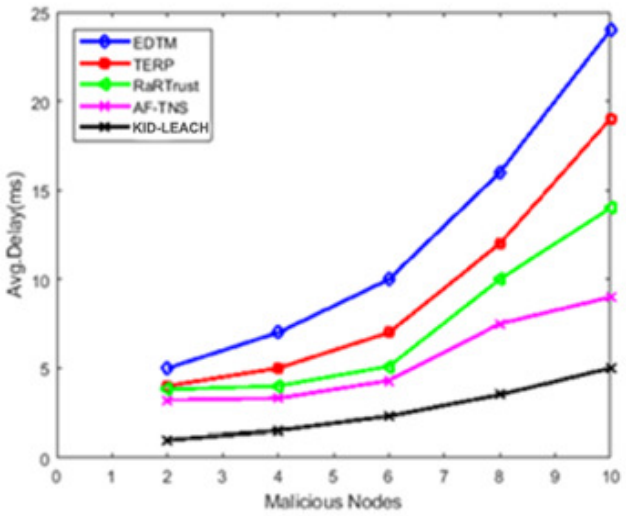

Figure 2. Average Delay Analysis

The Figure 2 shows the effect of vampire attack when average delay analysis is considered as a parameter. The numbers of nodes are varied and the results are taken. Average delay of KID-LEACH is very less when compared with the other existing protocols.

VII. CONCLUSION AND FUTURE SCOPE

Security during transmission and reception of data is very much essential in WSN. It is proved by simulation that Vampire attack results in more delay in forwarding packets. Experiments were conducted by varying the size of the network and we conclude that as far the network size increases the attack effects also increases. We have observed that the effect of vampire attack is less in KID-LEECH when compared to vampire attacks in other existing protocols. 94% efficiency is attained by using KID-LEECH protocol. We have also studied the root causes and the impact of various kinds of possible attacks in WSN. In future we plan to include more parameters to increase efficiency.

REFERENCES

1. Isaac Sajan, R, Jasper, J. Trust□based secure routing and the prevention of vampire attack in wireless ad hoc sensor network. *Int J Commun Syst*. 2020; 33:e4341. https://doi.org/10.1002/dac.4341
2. Kim, B. S., & Song, J. S. (2019). Energy-efficient and secure mobile node reauthentication scheme for mobile wireless sensor networks. *Eurasip Journal on Wireless Communications and Networking*, *2019*(1), [155]. https://doi.org/10.1186/s13638-019-1470-9.
3. Riaz, Muhammad & Attaullah, Buriro & A., Mahboob,. (2018). Classification of Attacks on Wireless Sensor Networks : A Survey. International Journal of Wireless and Microwave Technologies. 8. 15-39. 10.5815/ijwmt.2018.06.02.
4. Ali, S., Al Bulushi, T., Nadir, Z., & Hussain, O. K. (2018). Improving the resilience of Wireless Sensor Networks against security threats: A survey and open research issues. *International Journal of Technology*, *9*(4), 828-839. https://doi.org/10.14716/ijtech.v9i4.1526.
5. Tayebi A., Berber S.M., Swain A. (2015) Wireless Sensor Network Attacks: An Overview and Critical Analysis with Detailed Investigation on Jamming Attack Effects. In: Mason A., Mukhopadhyay S., Jayasundera K. (eds) Sensing Technology: Current Status and Future Trends III. Smart Sensors, Measurement and Instrumentation, vol 11.
6. Dewal P., Narula G.S., Jain V., Baliyan A. (2018) Security Attacks in Wireless Sensor Networks: A Survey. In: Bokhari M., Agrawal N., Saini D. (eds) Cyber Security. Advances in Intelligent Systems and Computing, vol 729. Springer, Singapore
7. Meenakshi Tripathi, M.S. Gaur, V. Laxmi, Comparing the Impact of Black Hole and Gray Hole Attack on LEACH in WSN, Procedia Computer Science, Volume 19, 2013, Pages 1101-1107, ISSN 1877-0509,https://doi.org/10.1016/j.procs.2013.06.155.
8. Virmani, Dr. Deepali & Soni, Ankita & Chandel, Shringarica & Hemrajani, Manas. (2014). Routing Attacks in Wireless Sensor Networks: A Survey.

9. Chan, H., Perrig, A. and Song, D., 2003, May. Random key predistribution schemes for sensor networks. In *2003 Symposium on Security and Privacy, 2003.* (pp. 197-213). IEEE.
10. Tseng, F., Chou, L. & Chao, H. A survey of black hole attacks in wireless mobile ad hoc networks. *Hum. Cent. Comput. Inf. Sci.* **1,** 4 (2011). https://doi.org/10.1186/2192-1962-1-4
11. Soomro, S.A., 2010. Denial of service attacks in wireless ad hoc networks. *Journal of Information & Communication Technology (JICT)*, *4*(2), p.10.
12. Pathan, A.S.K. & Lee, Hyung-Woo & Hong, Choong Seon. (2006). Security in wireless sensor networks: issues and challenges. 2. 6 pp. - 1048. 10.1109/ICACT.2006.206151.

