Review On Sinkhole Attack Detection and Prevention Approaches

[1]Shikha Saini, [2]Neetu Sagar
Department of electronic and communication engineering, Beant college of engineering and technology , gurdaspur, Punjab
([1]sainishikha27@yahoo.com)

Abstract- Wireless sensor network is a technology which provides the computation on low power and low energy and plays an important role in the field of technology. Most of fields like tracking, monitoring, surveillance, and environmental control use WSN for secure and effective communication. To fill all these requirements it needs better security features which protect the network from the attacks. Sinkhole attack in WSN weakens the computation and power. To detect the intruder in sinkhole attacks propose work is done in which algorithms analyze the suspected nodes by analyzing the consistency of data. Then, the intruder is recognized efficiently in the group by checking the network flow information.

Keywords- *WSN; sinkhole attack; security.*

I. INTRODUCTION

Wireless sensor network is used in various fields for the effective communication process in which user sends their information from one node to another node. Sometimes a user sends the secret information, data on the wireless network, it is very important to send this information very safely. In this network sensor nodes used wireless communication and it is easy to eavesdrop. The attacker can easily inject malicious messages into the network.

Types of Attacks in WSN

a) Grey Hole Attack: This attack is modification of black hole attack. In this attack attacker node behaves like a normal node for discovering route in the network. After it discovers the route then it drop the infected packets in network. This attack is difficult to detect because packet is dropped with certainty [4].

b) Wormhole Attack: In wormhole attack, the attacker can record the data packets at one location in the network and retransmit the data from another route of the data. Wormhole attack is a serious issue that occurred into the wireless sensor network. In the figure [1.1] the tunnel may be a wired link or wireless link between two nodes, this creates an illusion that the end point are very close to each other [2].

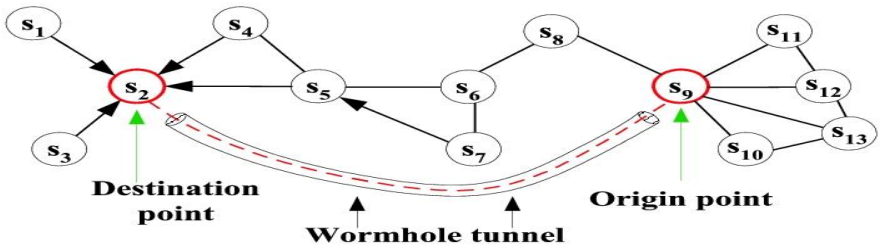

Fig.1.1: Wormhole Attack

A. Wormhole attack has two modes.

1) Hidden mode
2) Participation mode

c) Sink Hole Attack: in this attack incorrect information of the routing is send to the nodes as it is low cost and it provides proper destination node. Due to incorrect routing information it leads to packet loss and manipulation in original data packets. This attack disturbs all the network

process because nodes are sometime dependent on each other for information [4].

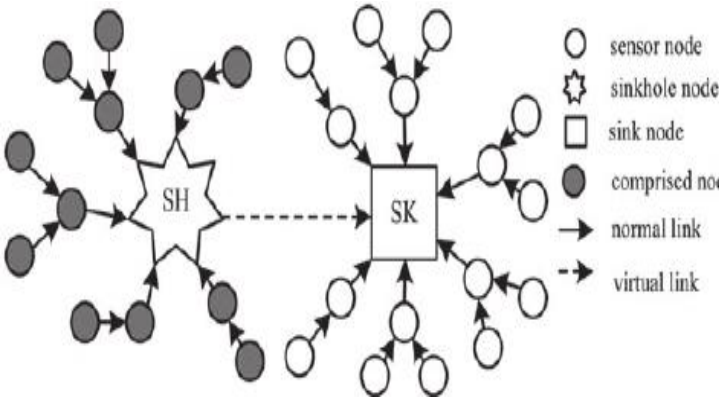

Fig. 1.2 :Sinkhole Attack

II. RELATED STUDY

Zhang, Zhaohui, et al. explained an energy efficient sinkhole detection approach which detects the malicious node effectively than the existing nodes. In this approach frequency of all nodes is established by m routes with optimal hops from per node to sink node. This method is based on the dynamic programming. This approach enhanced the detection rate and false positive rate [1]. Devibala, K., et al. proposed neighbor constraint traffic centric approach which is used to detect sinkhole attack and improve the quality of the WSN. It identifies the malicious node by the data send by neighbor node. It verifies the location of the node from where data is send to the node. This method provides sinkhole detection with high throughput and packet delivery ratio [2].

Mittal et al. proposed the major goal to analyze the effective protocol for the wireless sensor network. This analysis shows that the access control method and authentication methods are used in the WSN. This analysis shows that most of the approaches are based on the public key cryptography, which is the most expensive method. This paper provides a detailed comparative analysis of protocols with their advantages and disadvantages of each other [3]. Yasin, N. Mohammaed, et al. described the anomaly detection approach which detects the sinkhole attack in wireless sensor networks. This type of attack is not easy to detect due virtual path of the node. In this work Acceptance Acknowledgement approach is used to activate the digital signature system. This approach does not make any impact on the network and provides high detection rate of the malicious node [4].

Saghar et al. proposed the RAEED protocol which is used to detect the simple and intelligent tunnel attacks. This protocol helps to reduce the problem of DOS attack which disturbs the data routing and forward the data comes from the sink node. In future this work will be enhanced by applying formal methods to verify the communication issues [5]. Saghar et al. focused on the security issues of the wireless sensor network. It considers the Denial-of-Service attack on the data during the routing process. In this type of attack, the attacker attracts the traffic towards it and prevents the data from the neighboring node. This paper provides a protocol for the DOS attacks called as RAEED. It detects the simple and intelligent tunnel attacks very effectively [6].

Jan, Mian, et al. proposed a lightweight payload-based mutual authentication approach for a cluster based wireless sensor network. This is also called as PAWN approach. During the implementation process, it is implanted in two steps. First, the optimal percentages of the cluster heads are selected authenticated and allowed to communicate with the neighboring nodes. Second, each cluster head is in a role of server and provides the authentication to the nearby nodes. This scheme is validated with various schemes and the results show that if performed very well [7]. Kumar et al. proposed a localization algorithm which prevents from the Wormhole attack in the wireless sensor network. This algorithm is used to identify the unauthorized nodes by using the distance estimation method and Maximum Likelihood Estimation (MLE) to calculate the required location. The results in comparison show that this algorithm performed better than the existing algorithms [8].

Vidhya, et al. worked on the detection of sinkhole attack in AODV routing. This method uses energy power consumption in AODV and external energy by using battery. In this work MD5 algorithm is proposed for sink hole attack detection which prevent the network from the sever attack. This algorithm checks the energy transmitted by the node to the other nodes. This algorithm work effectively and enhance the packet delivery rate and throughput. It reduces the end to end delay in the network [9]. Jahandoust, et al. described the adaptive sinkhole aware algorithm in wireless sensor network. This work is based on the finding probability of affected nodes by sinkhole attack. In this the routing of the nodes is based on AODV protocols to route packets over the most reliable nodes. The subjective model identifies the behavior of the nodes in data receiving and sending. The behavior of whole network is observed by using probabilistic automation and captures the behavior of the network which is generated at the base station. The result of the proposed approach provides low packet loss rate and effective routing between the reliable nodes [10].

Inference from the literature review

Year	Author Name	Technique/ Algorithm used	Outcomes
2018	Zhang, Zhaohui,	Optimal route	In this approach

	et al	approach	frequency of all nodes is established by m routes with optimal hops from per node to sink node. This method is based on the dynamic programming. This approach enhanced the detection rate and false positive rate.
2018	Devibala, K., et al.	Mitigation Approach	It identifies the malicious node by the data send by neighbor node. It verifies the location of the node from where data is send to the node. This method provides sinkhole detection with high throughput and packet delivery ratio.
2017	Yasin, N. Mohammaed, et al	Authentication protocols	This analysis shows that the access control method and authentication methods are used in the WSN. This analysis shows that most of the approaches are based on the public key cryptography, which is the most expensive method.
2017	Saghar et al.	Anomaly Detection Approach	In this work Acceptance Acknowledgement approach is used to activate the digital signature system. This approach does not make any impact on the network and provides high detection rate of the malicious node.
2017	Saghar et al.	RAEED Protocol	This protocol helps to reduce the problem of DOS attack which disturbs the data routing and forward the data comes from the sink node.
2017	Jan, Mian, et al.	Payload-Based Authentication Approach	This paper provides a protocol for the DOS attacks called as RAEED. It detects the simple and intelligent tunnel attacks very effectively.
2017	Kumar et. al.	PAWN Approach	Proposed a lightweight payload-based mutual authentication approach for a cluster based wireless sensor network. This is also called as PAWN approach.
2017	Vidhya, et al.	MD5 Algorithm	This method uses energy power consumption in AODV and external energy by using battery. In this work MD5 algorithm is proposed for sink hole attack detection which prevent the network from the sever attack. This algorithm checks the energy transmitted by the node to the other nodes.

III. CONCLUSION

The propose paper presents the overview on the wireless sensor network and their issues with solution. The application of wireless sensor network is also discussed in this paper. The paper consists of introduction of WSN, Applications, hardware, layered architecture, types of attack its features and countermeasures. As a result effectiveness of the various approaches discusses in the tabular form which describes the technique and their outcomes on the wireless sensor network. This review helps a=to enhance the knowledge for research on the sinkhole attack and finding the effective algorithm from the past experiences.

REFERENCES

[1] Zhang, Zhaohui, et al. "M optimal routes hops strategy: detecting sinkhole attacks in wireless sensor networks." *Cluster Computing* (2018): 1-9.

[2] Mitigation approach for quality of service improvement in wireless sensor networks." *Industry Interactive Innovations in Science, Engineering and Technology*. Springer, Singapore, 2018. 357-366.

[3] Mittal, Vikas, Sunil Gupta, and Tanupriya Choudhury. "Comparative Analysis of Authentication and Access Control Protocols Against Malicious Attacks in Wireless Sensor Networks." *Smart Computing and Informatics*. Springer, Singapore, 2018. 255-262.

[4] Yasin, N. Mohammaed, et al. "ADSMS: Anomaly Detection Scheme for Mitigating Sink Hole Attack in Wireless Sensor Network." *Technical Advancements in Computers and Communications (ICTACC), 2017 International Conference on*. IEEE, 2017.

[5] Saghar, Kashif, Hunaina Farid, and Ahmed Bouridane. "Formally verified solution to resolve tunnel attacks in wireless sensor network." *Applied Sciences and Technology (IBCAST), 2017 14th International Bhurban Conference on*. IEEE, 2017.

[6] Vidhya, S., and T. Sasilatha. "Sinkhole Attack Detection in WSN using Pure MD5 Algorithm." *Indian Journal of Science and Technology* 10.24 (2017).

[7] Jahandoust, Ghazaleh, and Fatemeh Ghassemi. "An adaptive sinkhole aware algorithm in wireless sensor networks." *Ad Hoc Networks* 59 (2017): 24-34.

[8] Kalnoor, Gauri, Jayashree Agarkhed, and Siddarama R. Patil. "Agent-Based QoS Routing for Intrusion Detection of Sinkhole Attack in Clustered Wireless Sensor Networks." *Proceedings of the First International Conference on Computational Intelligence and Informatics*. Springer, Singapore, 2017.

[9] Saranya, P., Abin P. Varghese, and R. S. Balaji. "DETECTING AND PREVENTING THE WORMHOLE ATTACKS IN WIRELESS SENSOR NETWORK." *traffic* 3.04 (2017).

[10] Ma, Rui, et al. "Defenses Against Wormhole Attacks in Wireless Sensor Networks." *International Conference on Network and System Security*. Springer, Cham, 2017.