International Journal of Engineering & Technology, *7 (2.4) (2018) 157-160*

SPC

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET

Research Paper

Impact of Selective Forwarding attack on AODV Routing Protocol in Mobile Wireless Sensor Networks

Harkesh Sehrawat [1], Yudhvir Singh [1], Vikas Siwach [*1]

[1] Department of CSE, UIET, MDU, Rohtak
**Corresponding author E-mail: singhvikashuiet@gmail.com*

Abstract

wireless sensor network is the growing field of research having capacity to help the mankind with its usage in varied areas like military surveillance, medical etc. However these networks are vulnerable to certain attacks like black hole, wormhole and selective forwarding. In this paper selective forwarding attack is analyzed on varying number of attacker nodes and its impact on different performance parameters. It is concluded that the performance of the entire network is degraded with the increase in the number of malicious nodes.

Keywords: *WSN; Mobile WSN; Selective Forwarding Attack; AODV*

1. Introduction

The development in wireless technology and digital electronics has led to the development of Wireless sensor networks [1]. These WSN's are built up using various sensor nodes which possess the capability of sensing, processing as well as communicating the data. These nodes work in collaboration for producing desired functionality.

It is an emerging area with great potential to serve the mankind. The numerous solicitations [2] [3] are in the field of military surveillance, environment monitoring, healthcare etc.

The size or number of nodes are contingent upon the usage. The placement of these nodes need not be predetermined. Hence, the protocols used in these should be adaptive in nature. The usual standard is 2.4 GHz radios working on IEEE 802.15.4 or 802.11 or proprietary radius using 900 MHz.

Sensor Nodes: These are the major constituent of the WSN [4].They possess

1) A radio, which is used for the transmission of signals.
2) 2A micro controller for processing of data.
3) A sensor interface for sensing of data.

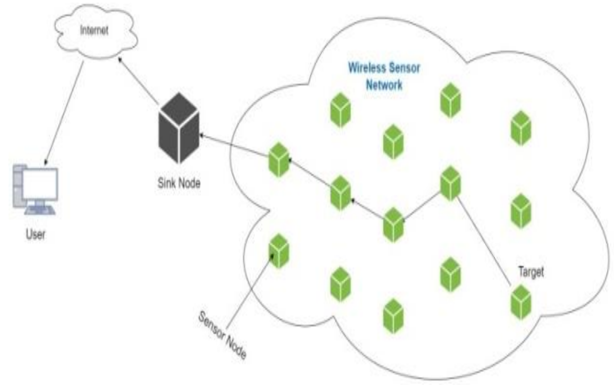


Fig. 1: Architecture of WSN.

4) Battery for power usages.

Topology of WSN: WSN usually follows follows mainly three different types of topologies. These are:

1) Star Topology: In this each sensor node is connected directly to the gateway.
2) Mesh Topology: In this type the sensor nodes are interconnected with each other and with the gateway
3) Cluster Tree Topology: Here the gateway act as the root node and each node is connected to another node at higher degree. Data flows from root to leaf.

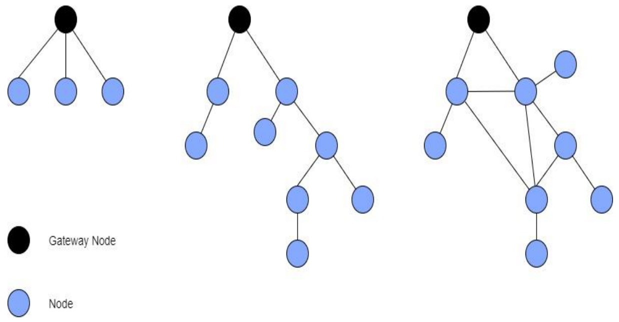


Fig. 2: Topology of WSN.

There are certain issues related with WSN's. The sensors node used are the tiny nodes with small batteries, hence our nodes should consume very less amount of energy. Due to this power constraint basic protocols can't be use in these networks. Due the broadcast nature of WSN, nodes are susceptible to numerous sorts of attacks.

Attacks in Wireless Sensor network

1) Selective Forwarding Attack [5]: In this attack the malicious node refuse to forward certain packets. It drops some packets and forwards some. This attack is difficult to find, as drop rate is high in WSN's so we may not be able to confuse it as normal packet drop.
2) Black Hole Attack [6]: In this attack, the malicious node drops all the packets passing through it.

3) Wormhole Attack [7]: In this attack, a malicious node tunnels message received in one part of network over a low latency link and replays the message in a different part.
4) Sybil Attack [8]: In this attack, a malicious node assures multiple identities at a time. Using 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, dispersity and multi path.
5) Jamming: Here the radio channel is disturbed by sending useless information.
6) Exhaustion: Here the victim node’s resources energy are consumed by obliging it do unnecessary calculations.

2. Selective forwarding attack

It [9] is an attack on network layer in WSNs. Usually in WSNs, sensor nodes forward data packets to next or neighboring sensor nodes keeping a “trust factor” that packets will reach their destinations at the end. The malicious nodes are setup by intruders which imitates as sensor node of the network thereby dropping out data packets which pass through them and forward only selective packets to the next sensor node. In this attack, when all the packets are dropped out, it is termed as black hole attack solely. Black hole attack is easy to detect as it drops all the incoming packets which gives clear indication of presence of a malicious node. But in selective forwarding, it is hard to detect these attacks as losing of few data packets is a normal phenomenon in network transmission.

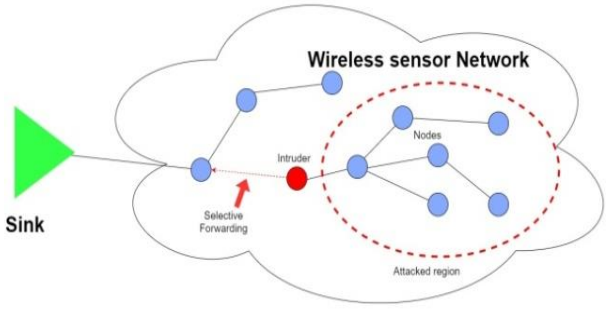
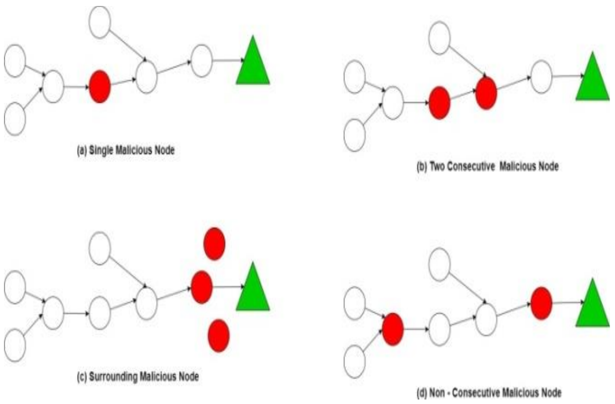


Fig. 3: Selective Forwarding Attack.

Classification of Selective Forwarding Attack

On the bases of malicious node: Selective forwarding attack can be categorized based on the arrangement of malicious nodes within the network. Figure 4 given ahead illustrating it.


(a) Single Malicious Node

(b) Two Consecutive Malicious Node

(c) Surrounding Malicious Node

(d) Non - Consecutive Malicious Node

Fig. 4: Classification of Selective Forwarding Attack.

On the bases of dropped packets: On the basis of packets dropped by the malicious nodes, this attack can be classified into three types:

a) All packets dropped received froma specific node in the network.
b) Packets dropped of a specific type.
c) Packets dropped randomly

3. Related work

Hung-Min Sun et al. [9] proposed a countermeasure method for sensing “Selective forwarding attack” in WSNwhich they named as a multi-dataflow topology (MDT). This method divides sensor nodes into two-dataflow topologies which can span over entire monitored region due to which base station necessitates information from either of the two topologies of the entire sensor network. This permits base station to retrieve accurate report even if any malicious node exists in any of the two topologies. The outcome demonstrates that MDT methods effectively expel the harm caused by the selective forwarding attacks. The principal advantage of MDT scheme is that base station can receive the data on time. Another advantage of this scheme is that MDT is very simple and lightweight in nature. The MDT procedure protects the selective forwarding attacks as well as other attacks.

Lim and Huie [10] have explored a countermeasure to selective forwarding attack for effectively sensing the forwarding conduct of malicious nodes. They first examined various adversarial situations based on implicit knowledge. They have proposed a hop-by-hop Cooperative detection method to detect the malicious nodes as well as mitigate their effects. With this scheme, the forwarding misbehavior of adversary nodes is reduces considerably and attains above 95% packet delivery ratio.

Liu et al. [11] put forwarded a Per-Hop Acknowledgement (PHACK) technique which is easy to implement and proved to be resilient against selective forwarding attack. In this technique, every intermediate node on the forwarding route sends an acknowledgement to source node through different routes which makes this scheme is more capable of identifying suspected malicious nodes. Moreover, this scheme is capable of quick recovery when routing fails. The compromised data can be rerouted through different paths to the sink node thereby leaving the suspected nodes. A crucial problem in such scheme is about the network lifetime which gets augmented due to the generation of more acknowledgements. However, the PHACK scheme only intensifies the energy intake in non-hotspot regions and there is no change in energy consumption in hotspot regions

Chawla and Sachdeva [12] discussed about selective forwarding attack on LEACH protocol. They analyzed and measured the impact of attacks by comparing the results with LEACH and without LEACH protocol. They have presented a detection scheme to identify malicious nodes in the network. They discussed about the hierarchical nature of LEACH protocol which works in two phases: setup phase and steady phase. Their work is divided in four steps. In first step, LEACH protocol is analyzed with various performance metrics. In second step, LEACH is analyzed with the presence of selective forwarding attack under some performance metrics. In next step, the impact of attack is measured. In the last step, a detection strategy is implemented for the identification of malicious nodes in the network. The simulation results using NS2 showed a huge drop in the packet delivery ratio.

Ren et al. [13] proposed a channel-aware reputation system to expose selective forwarding attack in WSNs. The system is based on adaptive detection threshold (CRS-A) which assesses the data forwarding nature of sensor nodes.

4. Proposed work

Here analysis of a wireless sensor network carried out in the presence of selective forwarding attack and its effect on different parameters such as end to end delay, jitter, Throughput etc. Here a mobile environment with 50 nodes and a varying number of 2 to 10 malicious nodes are taken for analysis using have used qualnet and Microsoft visual studio.

5. Result and analysis

We have used the qualnet 7.3.1 with 50 mobile nodes of maximum speed 10 m/sec in area of 1500 * 1500 m. The protocol used is AODV and 10 Zigbee applications are used.

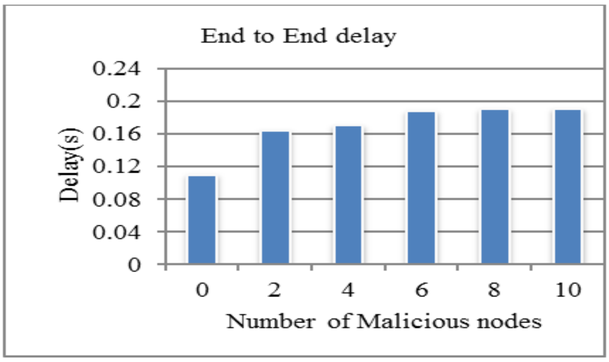


Fig. 5: End To End Delay.

As shown in figure 5 as the number of malicious nodes increases the End to End delay also increases. The overall performance of the system deteriorates with increase in number of malicious nodes in wireless senor network.

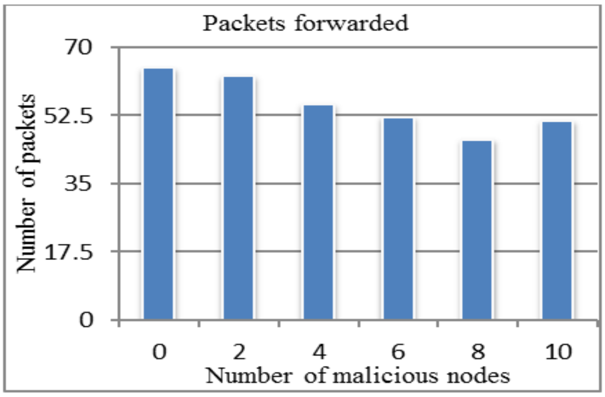


Fig. 6: Packets Forwarded.

In figure 6 above the effect of selective forwarding attack on packets forwarded is shown. Here as the number of malicious nodes gets increased the the numbers of packets forwarded get decreased. Hence lesser number of the packets forwarded, worse is the network performance.

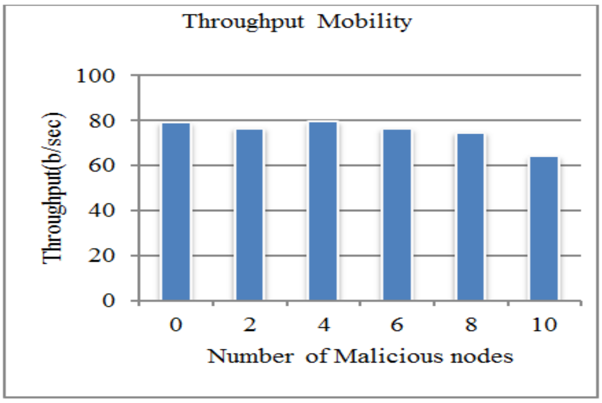


Fig. 7: Throughput.

As shown in figure 7 above, increase in count of malicious nodes decrease the throughput of the system. Also, as we have seen as the end to end delay and packets forwarded gets decreased the throughput of the WSN automatically decreased.

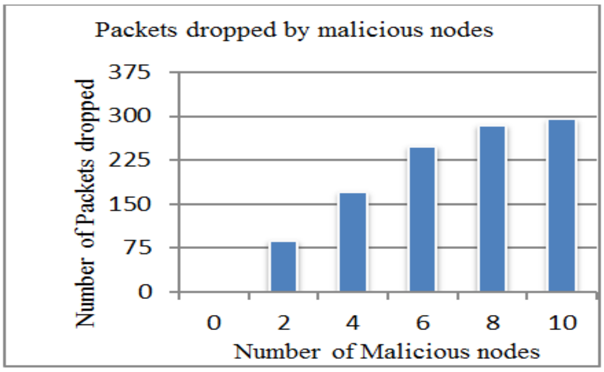


Fig. 8: Packets Dropped by Malicious Node.

As shown in figure 8 above, as the malicious nodes gets increased the number of packets dropped by them also increases. The increase is steady and almost linear.

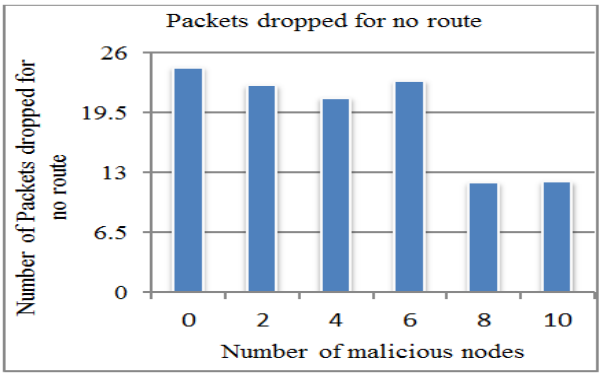


Fig. 9: Packets Dropped for No Route.

As shown in figure 9 above, There are no drastic change in the values and only decline in number of packets dropped due to no route available is reported.

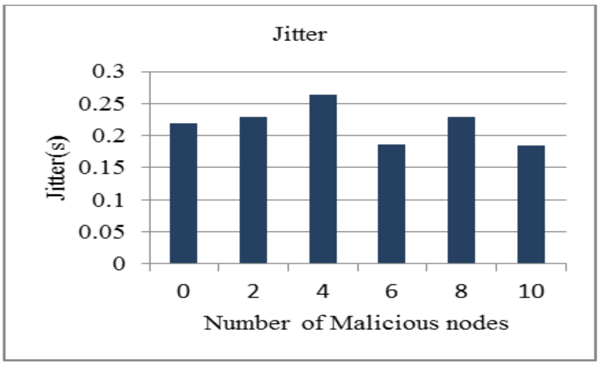


Fig. 10: Jitter.

As shown in figure 10 above, there is no major effect of attack on jitter.

6. Conclusion

In a selective forwarding attack, the malicious nodes drops or forwards the packets selectively. Here the attack is performed successfully and its impact is analyzed on different parameters. It is concluded that that as the number of malicious nodes is increased, the performance of system is also deteriorated. In future we will devise an algorithm for the detection of these attacks.

References

[1] Habib, “Sensor Network Security Issues at Network Layer,” in 2nd International Conference on Advance in Space Technologiees (IC-AST 2008), 2008, pp. 58–63.

[2] D. Virmani, A. Soni, S. Chandel, and M. Hemrajani, “Routing Attacks in Wireless Sensor Networks: A Survey,” arXiv Prepr. arXiv1407.3987, 2014.

[3] T. Kavitha and D. Sridharan, “Security Vulnerabilities In Wireless Sensor Networks : A Survey,” J. Inf. Assur. Secur., vol. 5, pp. 31–44, 2010.

[4] E. C. H. Ngai, J. Liu, and M. R. Lyu, “On the intruder detection for sinkhole attack in wireless sensor networks,” in IEEE International Conference on Communications, 2006, vol. 8, pp. 3383–3389.

[5] J. Brown and X. Du, “Detection of selective forwarding attacks in heterogeneous sensor networks,” IEEE Int. Conf. Commun., pp. 1583–1587, 2008.

[6] I. Krontiris, T. Dimitriou, and F. C. Freiling, “Towards Intrusion Detection in Wireless Sensor Networks,” in Proceedings of the 13th European wireless conference, 2007, pp. 1–10.

[7] L. Sharif and M. Ahmed, “The Wormhole Routing Attack in Wireless Sensor Networks (WSN),” J. Inf. Process. Syst., vol. 6, no. 2, pp. 177–184, 2010.

[8] S. Chen, G. Yang, and S. Chen, “A security routing mechanism against Sybil attack for wireless sensor networks,” in 2010 International Conference on Communications and Mobile Computing (CMC 2010), 2010, pp. 142–146.

[9] H. M. Sun, C. M. Chen, and Y. C. Hsiao, “An efficient countermeasure to the selective forwarding attack in wireless sensor networks,” in IEEE Region 10 Annual International Conference, TENCON 2007, 2007, pp. 4–7.

[10] S. Lim and L. Huie, “Hop-by-Hop cooperative detection of selective forwarding attacks in energy harvesting wireless sensor networks,” 2015 Int. Conf. Comput. Netw. Commun., pp. 315–319, 2015.

[11] A. Liu, M. Dong, K. Ota, and J. Long, “PHACK: An efficient scheme for selective forwarding attack detection in WSNs,” Sensors, vol. 15, no. 12, pp. 30942–30963, 2015.

[12] P. Chawla and M. Sachdeva, “Detection of Selective Forwarding (Gray Hole) Attack on LEACH in Wireless Sensor Networks,” Adv. Intell. Syst. Comput., pp. 389–398, 2017.

[13] J. Ren, Y. Zhang, K. Zhang, and X. Shen, “Adaptive and channel-aware detection of selective forwarding attacks in wireless sensor networks,” IEEE Trans. Wirel. Commun., vol. 15, no. 5, pp. 3718–3731, 2016.