Misdirection Attack in WSN: Topological Analysis and an Algorithm for Delay and Throughput Prediction

Roshan Singh Sachan[1], Mohammad Wazid[2], D.P. Singh[3], Avita Katal[4] and R.H. Goudar[5]
Department of CSE, Graphic Era University Dehradun, India
E-mail: [1]rsachan28@gmail.com; [2]wazidkec2005@gmail.com; [3]devesh.geu@gmail.com; [4]avita207@gmail.com; [5]rhgoudar@gmail.com

Abstract—*Wireless Sensor Network (WSN) has a great potential to be deployed in wide range of applications like consumer, industrial and defense sectors. WSNs are susceptible to various attacks, in which misdirection a kind of Denial of Service (DoS) attack is very difficult to detect and defend. In misdirection attack, the intruder misdirects the incoming packets to a node other than the intended node. Due to this attack, high end- to- end delay (sometimes infinite) is introduced in the network and performance of the network (i.e. throughput) is degraded. In this paper we have done a topological analysis of WSN in the presence of misdirection attack and presented an algorithm for the prediction of delay and throughput. We observed that WSN performs better for tree network topology as compared to mesh topology.*

Keywords: Misdirection Attack, Algorithm for Delay and Throughput Prediction, End-to-End Delay, Throughput.

I. INTRODUCTION

Wireless sensor nodes are low power electronic devices, deployed in remote areas, where power resources are limited. The demand of wireless sensor networks (WSN) has extended to too many real world applications such as habitat monitoring, environment monitoring, military surveillance, etc. Sometime the sensitive data is communicated to the destination node through an insecure medium. Thus, WSN can be easily attacked by Denial-of-Service (DoS) attacks, which sacrifices the information as well as causing large energy expenditure. Therefore, securing the links is important in designing a sensor network. In misdirection attack the attacker routes the packet from its children to other distant nodes, but not necessarily to its legitimate parent. This produces long delay in packet delivery and decreases the throughput of the network. Section 2 includes the literature review about different kinds of work done by the various authors related to misdirection (DoS) attack. The novelty of the proposed idea is discussed in section 3. In section 4 a brief introduction to Misdirection attack is given. Section 5 describes about various network topologies used in WSN. The simulation scenario for misdirection attack is discussed in section 6. In section 7 we have discussed performance evaluation followed by conclusion, future work and applications in section 8.

II. LITERATURE REVIEW

In paper [1] authors design a novel message observation mechanism (MoM) to detect and defense the DoS attack. Based on the spatiotemporal correlation, MoM utilizes the similarity function to identify the content attack as well as the frequency attack. The MoM adopts rekey and reroute countermeasures to isolate the malicious node. The security analysis shows that their solution not only detects and defenses the DoS attack but also can reduce the energy consumption. In paper [2] a new method is invented for discovering the misdirection attack. Produced results show that the misdirection attack causes consumption of network resources. The advantage of this work is to show the importance of reducing energy and time consumption as they are very significant in data transmission and reducing them makes transmission process more efficient and reliable. Paper [3] proposes TARF, a trust-aware routing framework for WSNs, to secure multi-hop routing in WSNs against intruders exploiting the replay of routing information. With the idea of trust management, TARF enables a node to keep track of the trust worthiness of its neighbors and thus to select a reliable route. Not only does TARF circumvent those malicious nodes misusing other nodes' identities to misdirect network traffic, it also accomplishes efficient energy usage. A new method has been invented in paper [5] for discovering the misdirection attack. The advantage of this work is to show the importance of reducing energy and time consumption. As these two factors are very significant in data transmission and reducing them make transmission process more efficient and reliable. Paper [8] depicts that we can defeat many threats using existing encryption and authentication mechanisms and other techniques can alert network administrators of ongoing attacks or trigger techniques to conserve energy on affected devices. Paper [9] provides a qualitative analysis of how proactive and reactive protocols cope with malicious internal attacks (i.e. misdirection attack) and whether one type of protocol offers inherently better resistance to the various attacks than the other.

978-1-4673-4603-0/12/$31.00 ©2012 IEEE

III. Problem Definition and Novelity

In order to find out for which network topology WSN performs better, we have done a topological analysis of the network in the presence of misdirection attack. To predict delay and throughput in the presence of misdirection attack, a delay and throughput prediction algorithm is designed for analyzing the performance of WSN in the presence of misdirection attack. In simulation the calculation of WSN performance parameters i.e. End-to-end delay and Throughput is done for different network topologies of WSN to find out which topology works best in presence of misdirection attack.

IV. Misdirection Attack Inside WSN

It is the most popular denial of service attack. This attack can be performed in different ways. A malicious node could deny a valid route to a particular node thereby denying service to the destination.

Misdirection attack can be performed in two ways:

A. Packets Forwarded to a Node Near to the Destination

This kind of misdirection attack is less intense, because packets reach to the destination but from a different route which further produces long delay, thus decreasing throughput of network (bit transfer per second).

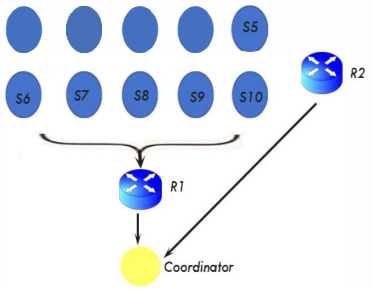

Fig. 1: Normal Flow of Packets

Figure 1 shows normal flow of packets.

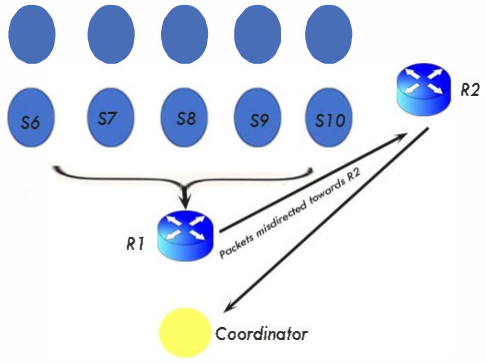

Fig. 2: Flow Packets when R1 becomes Attacker

Figure 2 shows the flow of packets; they are misdirected to node R2 by the malicious node R1.

We have simulated this attack.

B. Packets Forwarded to a Node Far Away from the Destination

This kind of misdirection attack is very harmful because all packets are forwarded to a node far away, preventing them to reach the destination so packets will not reach destination. Due to the attack the delay becomes infinite and further results in zero throughput.

Hence misdirection attacks are harmful in nature as they cause degradation in the performance of network.

C. Algorithm for Delay and Throughput Prediction for Misdirection Attack

IF packets forwarded to a node nearer to the destination THEN

$$delay_{predicted} \leftarrow delay_{normal} + \Delta_{delay};$$

$$throughput_{predicted} \leftarrow throughput_{normal} - \Delta_{throughput};$$

OTHERWISE

$$delay_{predicted} \leftarrow \infty;$$

$$throughput_{predicted} \leftarrow 0;$$

Δ_{delay} is the amount of time increased and $\Delta_{throughput}$ is the amount of throughput decreased due to misdirection attack.

V. Topologies in WSN

In WSN four network topologies used which are as follows:

A. Tree

In tree networks there is a central hub called a Root node which acts as main communication router. Central hub lies one level down from the Root node in the hierarchy. The lower levels form Star network. The Tree network can be considered a hybrid of both the Star and Peer to Peer networking topologies [11].

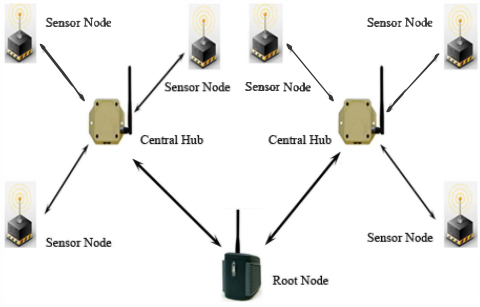

Fig. 3: Tree Network Topology inside WSN

Figure 3 shows tree network topology. Sensor nodes are reporting to central hubs which are further reporting to root node (coordinator of the WSN).

B. Mesh

Mesh networks allow data to "hop" from node to node, allowing the network to be self-healing in nature. Each node is able to communicate with each other as data is routed from node to node until it reaches the desired location. This type of network is one of the most complex and causes a significant amount of money to be used to deploy it properly [11].

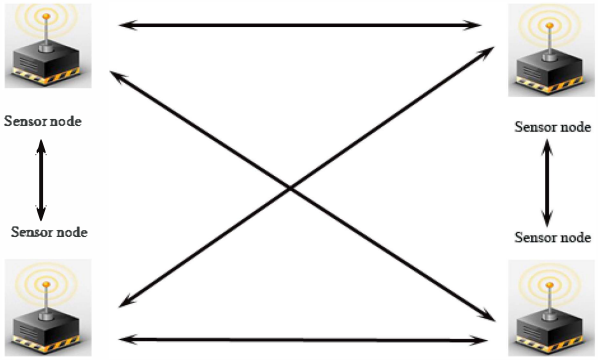

FIG. 4: MESH NETWORK TOPOLOGY INSIDE WSN

Figure 4 shows mesh network topology, sensor nodes are communicating directly to each other without any central hub or router.

C. Star

Star networks are connected to a centralized communication hub. As nodes cannot communicate directly with one another; all communications must be routed through the centralized hub. Each node acts as a "client" while the central hub is the "server" [11].

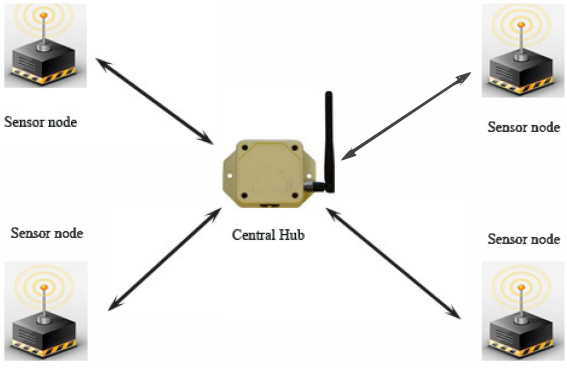

FIG. 5: STAR NETWORK TOPOLOGY INSIDE WSN

Figure 5 shows star network topology. The sensor nodes are communicating to each via central hub.

D. Peer-to-Peer

In Peer-to-Peer networks each node communicates directly with another node without going through a centralized communication hub unlike in star network topology. Each Peer device functions as both a "client" and a "server" to the other nodes in the network [11].

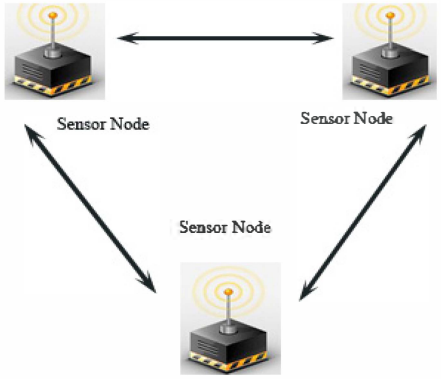

FIG. 6: PEER-TO-PEER NETWORK TOPOLOGY INSIDE WSN

Figure 6 shows peer-to-peer network topology. The sensor node is communicating to its one hop neighbor directly.

VI. SIMULATION SCENARIO OF MISDIRECTION ATTACK IN WSN

A. Simulation Scenarios

To verify this work we simulate a wireless sensor network (WSN) under misdirection attack. We have used the following two simulation scenarios in this paper:

FIG. 7: WSN WITH NORMAL FLOW

Figure 7 shows normal flow of packets. In this scenario we have considered ten sensor nodes (i.e. S1, S2 etc), two routers (i.e. R1, R2). Under normal flow all sensor node are reporting to router R1 and router R1 is reporting to the coordinator.

FIG. 8: WSN UNDER MISDIRECTION ATTACK

Figure 8 depicts misdirection attack. In this scenario we have again considered ten sensor nodes (i.e. S1, S2 etc), two routers (i.e. R1, R2). Under misdirection attack the packets which are coming to router R1 are misdirected to router R2. The malicious node R2 is shown in red label.

B. Experiment Design Parameters

Common Parameters

TABLE 1: COMMON PARAMETERS USED IN SIMULATION

Parameter	*Value*
Platform	Windows XP SP2
Simulator	Opnet modeler 14.5
Area	500 × 500 met (Fix)
Network Size	10 Sensor Nodes
	2 Routers
	1 Coordinator
Topologies	Tree, Mesh
Simulation Time	30 Minutes

Other Parameters

TABLE 2: OTHER PARAMETERS USED IN SIMULATION

Parameter	*Value*
Packet Inter- Arrival Time (sec)	Constant (1)
Packet Size (bits)	Constant (1024)
CSMA/CA Parameters	Default
Sensing duration (sec)	0.1
Physical Layer Parameters	Default

Implementations of Misdirection Attack

Under normal flow all sensor nodes are sending packets to router R1 which further sends them to coordinator. Router R2 is also reporting to coordinator. When misdirection attack occurs router R1 becomes attacker and starts misdirecting coming packets towards Router R2. Router R2 is also in the communication range of coordinator so all packets ultimately reach at coordinator but with some delay and reducing throughput. We have simulated this work for both topologies i.e. Tree and Mesh.

C. Results

In simulation we have taken following statistics of the network: End-to-end Delay (msec), Throughput (bps).

TABLE 3: END-TO-END DELAY

	Tree Topology		*Mesh Topology*	
	Normal Flow	*Attack*	*Normal Flow*	*Attack*
End-to-end Delay (msec)	17.77	19.05	19.76	24.69

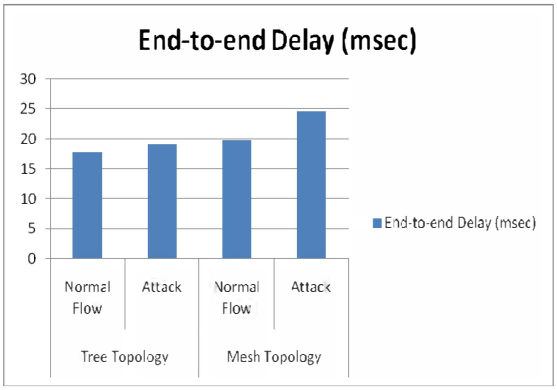

FIG. 9: END-TO-END DELAY (MSEC)

Figure 9 shows end-to-end delay (msec) with normal flow and also in the presence of attack with both topologies.

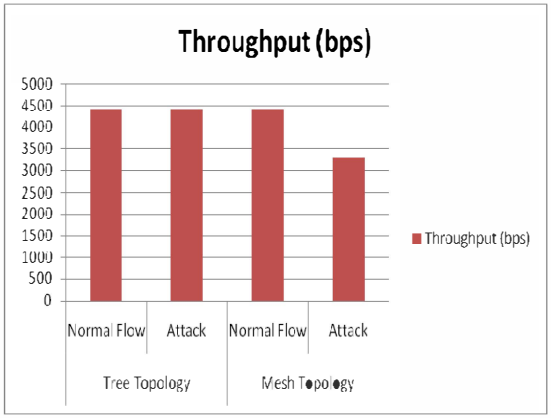

FIG. 10: THROUGHPUT (BPS)

TABLE 4: THROUGHPUT

	Tree Topology		*Mesh Topology*	
	Normal Flow	*Attack*	*Normal Flow*	*Attack*
Throughput (bps)	4425.64	4421.19	4424.7	3319.47

Figure 10 shows throughput (bps) with normal flow and also in the presence of attack for both topologies.

TABLE 5: Δ DELAY

	Tree Topology	*Mesh Topology*
Increment in Delay (msec)	1.28	4.93

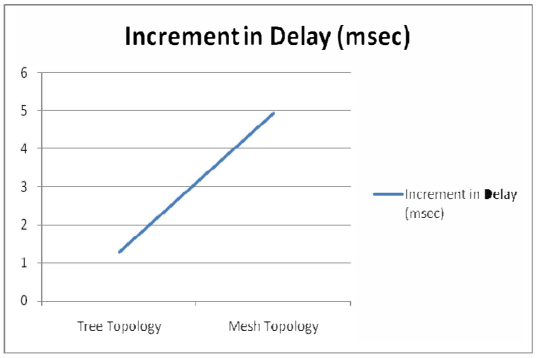

FIG. 11: INCREMENT IN DELAY (MSEC)

Figure 11 shows increment in delay (msec) in the presence of misdirection attack.

TABLE 6: Δ THROUGHPUT

	Tree Topology	*Mesh Topology*
Decrement in Throughput (bps)	4.45	1105.23

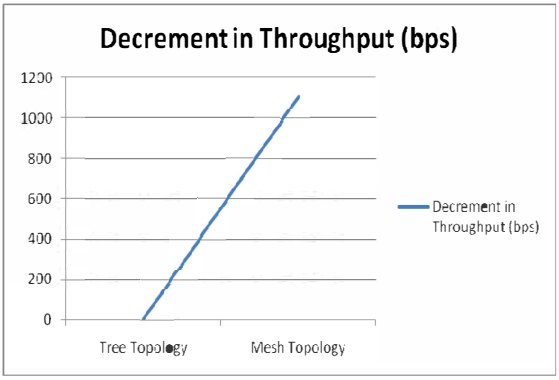

FIG. 12: DECREMENT IN THROUGHPUT (BPS)

Figure 12 shows decrement in throughput (bps) in the presence of misdirection attack.

VII. PERFORMANCE EVALUATION

Here, we try to evaluate the performance of a WSN in the presence of misdirection attack. Some of the observations are:

- End-to-end delay of the network increases for both topologies. In case of tree topology it goes 17.77 to 19.05 msec and for mesh it goes 19.76 to 24.69 msec (Refer Table III).
- Throughput of the network decreases for both topologies. In case of tree topology it goes 4425.64 to 4421.19 bps and for mesh it goes 4424.70 to 3319.47 bps (Refer Table VI).

VIII. CONCLUSION

- The existence of misdirection attack affects both parameters of network i.e. End-to-end delay and Throughput of network which in turn degrades the performance of network. We observed that in the presence of misdirection attack the increment in delay (Δ_{delay}) is 1.28 msec for tree topology and for mesh topology it is 4.93 msec. The decrement in throughput ($\Delta_{throughput}$) is 4.45 bps for tree topology and 1105.23 bps for mesh topology. Hence we observed that the performance of WSN is better in tree topology as compared to mesh topology in case of misdirection attack.
- In future this can be extended with varying number of attackers, node density and system size.
- The application of this work is in defense sector where the chances of occurrence of misdirection attack are high.

ACKNOWLEDGMENTS

We are very thankful to all those people, who guided and supported us. Without their valuable guidance and support, this task was not possible.

REFERENCES

[1] Yi-ying ZHANG, Xiang-zhen LI, Yuan-an LIU, "The detection and defence of DoS attack for wireless sensor network" , Elsevier Journal of China Universities of Posts and Telecommunications, Volume 19, Supplement 2, October 2012, Pages 52-56.

[2] Syed Omar, Tariq Saleh, Al-Khalidy, "Design an Algorithm To Discover The MisdirectionAttack For Increasing The Life Time in ComputerNetwork", International Journal of Computer Science and Information Security (IJCSIS), vol. 9, No. 1, December 2011.

[3] Guoxing Zhan, Weisong Shil, Julia Deng, "TARF: A Trust-Aware Routing Framework for Wireless Sensor Networks", EWSN 2010, LNCS 5970, pp. 65–80, 2010.

[4] Hailun Tan, Diethelm Ostry, John Zic, Sanjay Jha, "A Confidential and DoS-Resistant Multi-hop Code Dissemination Protocol for Wireless Sensor Networks", ACM WiSec'09, March 16–18, 2009.

[5] M. Y. Abdullah, Hua Gui Wei, N. Alsharabi, "Wireless sensor networks misdirection attacker challenges and solutions", IEEE International Conference on Information and Automation, 2008.

[6] Somanath Tripathy, Sukumar Nandi, "Defense against outside attacks in wireless sensor networks", Elsevier Computer Communications, Volume 31, Issue 4, 5 March 2008, Pages 818-826.

[7] An Liu, Young-Hyun Oh, Peng Ning, "Secure and DoS-Resistant Code Dissemination in Wireless Sensor Networks Using Seluge", ACM International Conference on Information Processing in Sensor Networks 2008.

[8] David R. Raymond, Scott F. Midkiff, "Denial-of-Service in Wireless Sensor Networks: Attacks and Defenses", Published by the IEEE CS no 1536-1268/08/ 2008.

[9] Po Wah Yau, Shenglan Hu, Chris J. Mithell, "Malicious attacks on ad hoc network routing protocols", International Journal of Computer Research Vol 15 Issue 1, 2007.

[10] Jing Deng, Richard Han, and Shivakant Mishra, "Defending against Pathbased DoS Attacks in Wireless Sensor Networks", ACM SASN'05, November 7, 2005.

[11] Wireless Sensor Network Topologies Available at <www. k5systems.com/TP0001_v1.pdf>