Impact Analysis of Network Layer Attacks in Real-Time Wireless Sensor Network Testbed

Navjot Sidhu[1]
Research Scholar
I. K. Gujral Punjab Technical University
Kapurthala, Punjab, India

Monika Sachdeva[2]
Associate Professor
I. K. Gujral Punjab Technical University
Kapurthala, Punjab, India

***Abstract*—With the rapid increase in the demand for Wireless Sensor Network (WSN) applications. The intrusive activities are also raised. To save these networks from the intruders it is required to understand the implications of any malicious act. Most of the researchers have utilized simulated software to understand the impact of such intrusions, however, real network conditions vary from the simulated environment. Therefore, the current work focuses on analyzing the impact of network layer attacks in real-time WSN testbed. The contributions of this work are threefold. Firstly, it presents the deployment of a real-time experimental testbed using standardized sensor devices in a multi-hop topological arrangement. Secondly, it provides the implementation details of seven network layer attacks: Blackhole (BH), Dropping Node (DN), Drop Route Request (DRREQ), Drop Route Reply (DRREP), Drop Route Error (DRERR), Grayhole (GH) and Sinkhole (SH) in a single testbed. Finally, the testbed performance with and without each attack is monitored and compared in terms of network performance metrics to understand the attacks' impact. This work will be helpful for the research community for proposing efficient attack detection and prevention solutions for these networks.**

Keywords*—Attack; impact; performance; real-time; Wireless Sensor Network (WSN)

I. Introduction

Wireless Sensor Network (WSNs) is a widely used technology in most of the monitoring applications nowadays. The common applications include security monitoring of homes, health monitoring in hospitals, traffic monitoring on roads, warehouse monitoring, weather monitoring, etc. The basic aim of all of its applications is to monitor the sensing environment and send the sensor readings to the base station so that the appropriate actions can be taken on time. Hence, data from the sensor nodes is quite important for mission-critical applications [1].

To achieve these applications' goals, the deployed sensor nodes should monitor the environment and communicate with other network devices timely. However, the intruders usually disrupt the normal network operations by launching intrusions in these networks. As a result of which, sensor nodes can not communicate with each other and the network performance degrades drastically. Hence, to prevent such networks from degradation, these attacks' impact should be monitored carefully.

However, most of the previous studies investigated the impact of a few intrusive activities by implementing the attacks in a simulated environment only. The simulation results vary drastically from the actual network performance. So, the simulated findings can not be directly applied to real life application scenarios.

For this work, to observe the network's actual performance with and without attack, the real-time WSN testbed is deployed for experimentation which presented a realistic performance measurement. For differentiating the behavior of the network under intrusive and legitimate activities, seven similar network layer attacks are implemented in the testbed. So, the majority of attacks at the network layer can be studied in a single study. The work successfully shows the impact of each attack in the testbed in terms of computed performance metrics.

This work can be of great value to understand such attacks in real-life applications. It can provide an insight for the developers to design secure sensor devices. Moreover, it can be used to introduce protective measures to prevent these networks from such critical attacks.

This paper is organized into the following sections: Section II describes the related literature work. Section III is an experimental methodology that defines the WSN testbed, the routing protocol used in the testbed, attack implementations, and performance metrics used. Section IV presents and discusses the results. Finally, Section V concludes the work.

II. Related Work

This section presents the overview of existing attack implementations and experimentation analysis in WSN.

Tripathi et al. [2] simulated the blackhole and grayhole attack in LEACH protocol based upon the energy threshold in NS-2 and compared the attack impact. The authors suggest the detection of such attacks at the base station by observing the cluster head node and its data transmission. Dini and Tiloca [3] presented a stimulative approach for attack impact analysis and ranked the attacks according to severity. The paper also analyzed separate countermeasures for each attack type. However, it is an extremely costly solution for resource-constrained networks. Riecker et al. [4] measured the impact of Denial-of-Service Attacks: Jamming and Blackhole, using a testbed consisting of TelosB motes. The authors identified the performance metrics classes based on their capability to detect attacks. They used the packet delivery rate as a metric to differentiate between attack and normal network behavior. However, the detection of attacks only by observing performance metrics is not appropriate as sometimes the specific network parameters show significant variation in metrics in case of normal traffic

scenarios. Therefore, the fluctuation of legitimate traffic can be misunderstood as an attack. Chaudhary and Thanvi [5] analyzed the performance of modified AODV protocol under the DoS attack in NS-2. The paper suggested attack detection based on the RREP sequence number attribute of packets. But, such attack specific solutions are not feasible to save the real networks from attacks. Almomani and Al-Kasasbeh [6] presented the impact analysis of DoS attacks in LEACH: Blackhole, Grayhole, Flooding attack, and Scheduling attack using NS-2. The paper showed the attack impact with a major drop in packet delivery ratio. Nevertheless, the LEACH is not a standardized protocol used in WSN hardware. Rupayan Das et al. [7] compared the effect of network and physical layer attacks in the AODV routing protocol. The attacks were simulated in OPNET 14.5 and attack impact was analyzed with quality of service parameters.

Ioannou and Vassiliou [8] implemented routing layer packet drop attacks and investigated the attack impact from the sink node and victim node using the COOJA simulator. The authors considered the variations in the network topology to study attack impact. The paper showed that using some network parameters the presence of attacks can be identified however, it did not state the type of attack. Diaz and Sanchez [9] proposed a simulator for performance analysis of three attacks with attacker modeling and attack simulation, and suggested to be used by developers to understand attack behavior and develop secure systems. The paper did not provide any strategy to identify a specific type of attack. Govindasamy and Punniakody [10] analyzed the performance of AODV, OLSR, and ZRP routing protocols in Qualnet 5.0 under wormhole attack only using performance metrics. Tomin and McCann [11] analyzed the network layer attacks deployed against the routing protocol for low-power and lossy networks (RPL) using the COOJA network simulator. The impact of attacks was shown using the packet delivery ratio and end-to-end delay. But, specific attack types cannot be identified from the performance metrics of a network. Baskar et al [12] simulated and analyzed the network performance under the sinkhole attack in WSN in terms of energy consumption, throughput, and packet delivery ratio. The authors concluded that in a network with a large number of network nodes and few attacker nodes, attack impact was less. However, there is no practical evidence of this conclusion. Rana and Kumar [13] provided a detailed analysis of the AODV routing protocol with and without the presence of malicious node in the network using Qualnet 5.0 simulator and analyzed the throughput, average jitter, and packet drop ratio. Gomez et al [14] implemented the wormhole attack in a ZigBee experimental framework using XBee S2C nodes to find signatures for detecting this attack in real environments.

To sum up, much of the preceding research was performed in a simulated environment to understand the impact of attacks in WSNs. Moreover, the majority of the earlier studies focused on considering merely one or two attack types at a time. But, the real-time network behaves differently than the controlled simulated network.

Therefore, the multiple related attacks are implemented in real network scenarios to study the detailed behavior of malicious activities. And, the behavior of these attacks as compared to legitimate network performance is analyzed. Besides, the proposed study used the standardized network devices to deploy the testbed for experimentation to create a real network similar to real-life application scenarios.

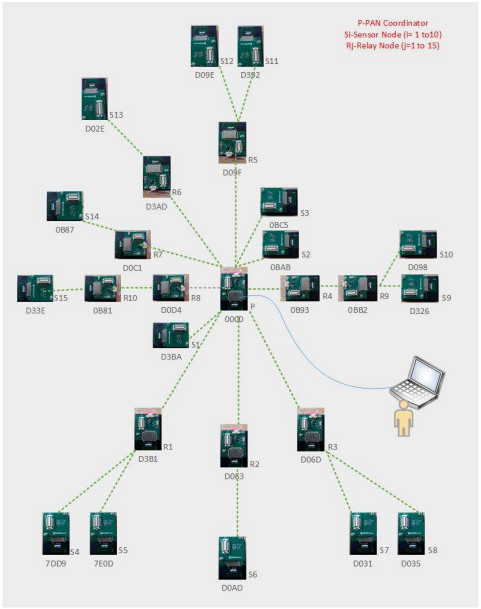

Fig. 1. WSN Testbed

III. Experimental Methodology

The experimental methodology comprises of the detail of the components of testbed, the routing protocol used, the definitions of attacks implemented, and performance metrics calculated.

A. WSN Testbed

Most of the research in the field of security of WSN is being done in a simulated environment. Some researchers preferred to use open-source network simulators and others proposed new WSN specific simulators. However, the actual network environment differs significantly from the simulated one. Therefore, the real WSN testbed is being deployed for experimentation.

To conduct the experiments, $SENSEnuts^{TM}$ wireless sensor kit is used. The kit consists of three main components. The wireless sensor module senses the light and temperature of the sensing environment. The radio module is responsible for creating a route between the source and the destination nodes. It connects the nodes at multi-hop distance. The Gateway module is connected with the laptop/desktop computer and responsible for sending the captured information to the computer using the SenseLive software. The SenseLive is a C based software that provides functionalities to the users like programming a sensor and radio node, displays the data sensed by sensor nodes in the form of user-defined tables, saves the data tables in database files, etc.

Fig. 1 shows the topological arrangement of Sensenuts nodes used to conduct experiments. The real network of 26 nodes includes 15 sensor nodes and 11 radio nodes. 1 radio node is programmed as the personal area network (PAN) Coordinator which manages the whole network, 10 as relay

Fig. 2. WSN Testbed in LAB

nodes/ coordinators which have routing capabilities and 15 sensor nodes as sensing devices. Si represents the sensor nodes, Ri shows the relay nodes and P is a PAN coordinator. MAC id of each node is mentioned against each node. All the sensor nodes and relay nodes are battery-operated devices. PAN is connected with the computer system through the gateway module and uses the computer power to operate in the network. Hence, the PAN of the network has the highest operating power as compared to other devices.

Each sensor node searches a route to the PAN of the network either directly at a 1-hop distance or through relay nodes at 2-hop and 3-hop distance when it has the data to transmit. The route between the sensor node and PAN is established through a ZigBee based routing protocol. After the route is formed, the sensed information is sent by the sensor nodes to the PAN. All the performance-related calculations are performed at PAN as it has maximum operating capacity in comparison to other limiting power devices. After calculations, the required results are communicated to the computer system and stored in forms of tables. Fig. 2 shows the WSN testbed deployed in real-time.

B. Routing Protocol

The Sensenuts WSN platform is based on ZigBee wireless standard [15] which uses Adhoc On Demand Distance Vector (AODV) Routing protocol [16] at the network layer. AODV uses mainly three control packets i.e. Route Request (RREQ), Route Reply (RREP), Route Error (RERR) to search, establish, and repair the routes between the devices. When a sensor node has data to send but does not have a route to the destination node, it broadcasts the RREQ packet in the network. The RREP packet is unicasted either by the destination node or by an intermediate node if it knows an active route to the destination node. In case of a link failure or a route error, a RERR packet is either unicasted or broadcasted by an intermediate node. The implementation of AODV protocol under normal network conditions as well as under each attack, is shown in algorithm 1.

C. Attack Implementation

In the current work seven network layer attacks are implemented: Black hole, Dropping Node, Drop RREQ, Drop RREP, Drop RERR, Gray hole, Sinkhole. To implement these attacks, the attack actions to launch each attack type and goals achieved by the attackers are identified [17]. The analysis shows that all of these routing layer attacks degrade the network performance and deplete the network resources. The implementation details of each attack type in real WSN test-bed is defined follows and implementation steps are described in algorithm 1:

1) Black hole Attack: For the implementation of the black hole attack [2], [18] when the attack node receives the RREQ message, it generates a false RREP message using a very high destination sequence number value to prove that it has a fresh route to the base station/destination. On the reception of the RREP message by the source node, it establishes a route through it based upon its highest value of destination sequence number field. When the sensed data is transferred through this route, the black hole node simply drops all the data packets. Therefore, when the route is formed through the black hole node, the information from the source node cannot reach to the destination.

2) Dropping Node Attack: The dropping node [18] does not launch any attack during route establishment like the black hole node. It simply waits for a route to be establish through it. When a route between a source and a destination node is established through the dropping node, it drops all the data packets.

3) Drop RREQ Attack: The drop RREQ attack [19] is implemented in a relay node as when the compromised node receives the RREQ message from its neighboring nodes, it simply drops the RREQ messages. This attack node either debars the route formation for neighboring source nodes or delays the route formation period.

4) Drop RREP Attack: The drop RREP node [19] drops the RREP message when received from any destination node or intermediate node. Therefore, the route is not established between two nodes.

5) Drop RERR Attack: For the implementation of drop RERR [19], when an attack node receives a RERR message, instead of forwarding, drops it. So that in case of any link failure and route error the corresponding processes cannot be initiated by the intended nodes.

6) Gray hole Attack: The Gray hole attack [2] is implemented as a variation of dropping node attack. It does not forcefully form any route through it. However, when a route for data transfer is formed through a Gray hole attack node, it launches a selective packet drop attack. The random packet drop is implemented for dropping data packets.

7) Sinkhole Attack: The Sinkhole attack [12], [20] is implemented as an extension to the Black hole attack. This attack node forces the destination node to send the RREP message through it. So, it changes the destination sequence number field of RREQ with a very high value and hop-count with a minimum value and broadcast RREQ towards the destination node. At the same time, it generates the RREP using a very high destination sequence number. Hence, the sinkhole node wins the route, and the detection of this node becomes difficult. After the route establishment, the attacker node randomly drops some of the data packets received from the sensor nodes.

The real-time experimentation is performed to capture the data from WSN testbed which is further used to analyze the malicious behavior during network communication. For analyzing the performance of WSN test-bed under attacks all

Algorithm 1 AODV operation under normal and attack conditions

$S \rightarrow SourceNode$
$D \rightarrow DestinationNode$
$I \rightarrow IntermediateNode$
$RT \rightarrow RouteTable$
$RREQ \rightarrow RouteRequestMessage$
$RREP \rightarrow RouteReplyMessage$
$RERR \rightarrow RouteErrorMessage$

Step 1: S checks RT entry for D.
Step 2: If (route exists)
{
Forward packets to next-hop.
}
Else
{
Initiates Route Discovery Process.
}

Route Discovery:
Step 1: S creates and broadcasts RREQ.
Step 2: I receives RREQ.
Step 3: If (I=Drop RREQ Node)
{
I drops the RREQ.
Exit
}
Else
{
If (D's sequence no in latest S'RREQ>D's sequence no in previous S'RREQ)
{
I sets up a Reverse Route Entry for S in its RT.
If (Route exists from I to D in I's RT)
{
If (D's sequence no in I's RT>=D's sequence no in RREQ)
{
I Creates RREP.
If (I= Sinkhole Node or Blackhole Node)
{
Set RREP.dst_seq_no= Higher value.
}
I unicasts RREP towards S.
}
}
Else
{
I increments hop count in RREQ.
If (I= Sinkhole Node)
{
Set RREQ.dst_seq_no= Higher value.
}
I broadcasts RREQ to its neighbors.
}
}
Else
{
Discard RREQ.
}
}

Step 4: RREQ reaches D, provided D is reachable from S.
Step 5: D creates RREP.
Step 6: D unicasts RREP towards S.
Step 7: I receives a RREP.
Step 8: If (I=Drop RREP Node)
{
I drops RREP.
Exit
}
Else
{
Sets up a Forward Route Entry to D in its RT.
I forwards the RREP towards S.
}

Data Transmission:
Step 1: S receives RREP.
Step 2: S starts packet transmission on route to D.
Step 3: I receives the data packets.
Step 4: If (I=Dropping Node or Blackhole Node)
{
Drop all the data packets.
}
Else If (I=Grayhole Node or Sinkhole Node)
{
Drop some of the data packets randomly.
}
Else
{
I forwards the data packets towards D.
}
End If

Route Maintenance:
Case I: S disconnects/moves from route established. S initiates a new route discovery.
Case-II: Either I or D disconnects/moves
Step 1: I creates RERR.
Step 2: I forwards RERR towards S.
Step 3: If (I=Drop RERR Node,receives RERR)
{
I drops RERR.
}
Else If (S receives RERR)
{
Delete route to D.
Initiates a new route discovery.
}
Else If (Another I receives RERR)
{
Delete route to D.
Forwards RERR towards S.
}
End If

TABLE I. NETWORK PARAMETERS

Parameters	Value
PAN Node	1
Relay Nodes	10
Sensor Nodes	15
Routing Protocol	AODV
Topology	Multi-hop (up to 3-hop distance)
Packet Size	6 Bytes
Packet Interval	1 sec
No of Packets Send	100
No of Attacker	01
No of Attacks Launched	07

network layer attacks are being implemented on the testbed. In the real network of 26 nodes, firstly the legitimate performance of the test-bed has been captured so that the comparison can be made in case of any intrusion in the network. After that, for each scenario, one relay node is programmed as an attack node and the behavior of the network is captured in terms of performance metrics. For calculating the results, each experiment is run five times so that real network efficiency can be observed. Table I summarizes the network parameters used for conducting experiments.

D. Performance Metrics

The following performance metrics for each sensor node are measured at PAN to compare the network performance with and without any attack.

1) Average Throughput (in bps): It is the average of the number of bits received from a sensor node to its data transmission duration.

$$Avg.Throughput = (No.of PacketsReceived * PacketSize)/Time \quad (1)$$

2) Packet Delivery Ratio (PDR): It is the ratio of the number of packets received at the base station from a sensor node to the number of packets sent by that sensor node.

$$PDR = (No.of PacketsReceived)/(No.of PacketsSent) \quad (2)$$

3) Number of Packets Received: It is the sum of the number of packets received at the base station from a sensor node.

4) Average Inter-arrival Time (IAT) (in secs): It is the average time difference between two consecutive packets when reached the base station from a sensor node.

$$Avg.IAT = (CurrentPacketTime - Previous PacketTime)/(No.of PacketsReceived) \quad (3)$$

All of the calculations are performed at the base station only as it has the highest battery power. The impact of each attack in terms of calculated performance metrics is presented in the form of graphs in the next section.

IV. RESULTS AND DISCUSSION

The results show the impact of each attack with respect to the legitimate network performance in terms of identified performance metrics.

1) Black hole Attack Analysis: Fig. 3(A) shows the impact of Black hole attack in the testbed in terms of average throughput. The average throughput lies between 32 to 49 bps in case of the legitimate network. However, when one relay node acted as black hole attacker, it affected majority of sensor nodes and resulted in zero bps average throughput of these sensor nodes. Because such sensor nodes could not connect with the base station during network formation and all of their data packets are dropped. Similarly, the PDR of these nodes as shown in Fig. 3(B), is also zero as all the data packets from these sensor nodes are dropped by the black hole attack node. It can be further verified from Fig. 3(C), which shows the number of packets from each sensor node reached at the base station. It is zero for the attack affected sensor nodes. Fig. 3(D) shows the average IAT, which is zero for the sensor nodes which could not be connect with the base station during the experimentation.

2) Dropping Node Attack Analysis: As shown in Fig. 4 sensor nodes 0B87, D035, and D326 are under the influence of the dropping node attack. The average throughput of these sensor nodes is zero bps as shown in Fig. 4(A). Also Fig. 4(B) and (C) are showing the PDR and number of packets received, respectively for these affected nodes that are also zero. The average IAT for those sensor nodes that could not communicate with the base station is also zero (see Fig. 4(D)).

3) Drop RREQ Attack Analysis: Fig. 5 shows the impact of Drop RREQ attack. Due to the presence of DRREQ attacker, two sensor nodes could not connect with the base station because the RREQ packets sent by these sensor nodes dropped by the attacker node. Therefore, the average throughput of these nodes is zero bps and average IAT is zero seconds. Also the route establishment of few nodes is delayed by DRREQ attack as a result of which less number of packets from those sensor nodes reached at the base station resulted in less or zero PDR and low packet received count.

4) Drop RREP Attack Analysis: As shown in Fig. 6, the impact of Drop RREP attack is either delayed route formation or no route between a sensor node and the base station. Average throughput of the affected sensor nodes is increased because such nodes are able to send less number of packets to the base station and most of their data packets are dropped while waiting for the route establishment. In Fig. 6(B) and (C), the PDR and number of packets received from the sensor nodes clearly shows the influence of DRREP attacker in the testbed.

5) Drop RERR Attack Analysis: Fig. 7 shows the impact of Drop RERR attack in the testbed. The DRERR attacker delayed the route repair in the network in case of a link failure. As a result of which less number of packets from the affected sensor nodes reach the base station and hence showing less PDR. The average throughput and average IAT for such sensor nodes are dropped due to delayed route repair and packet dropped during this period.

6) Gray Hole Attack Analysis: The Gray Hole attacker drops the data packets selectively therefore results in decreased average throughput, PDR, packet received count and increased average IAT of the affected sensor nodes. As shown in Fig. 8(A) the average throughput of two sensor nodes is decreased. Fig. 8(B) and (C) shows the decrease in PDR and

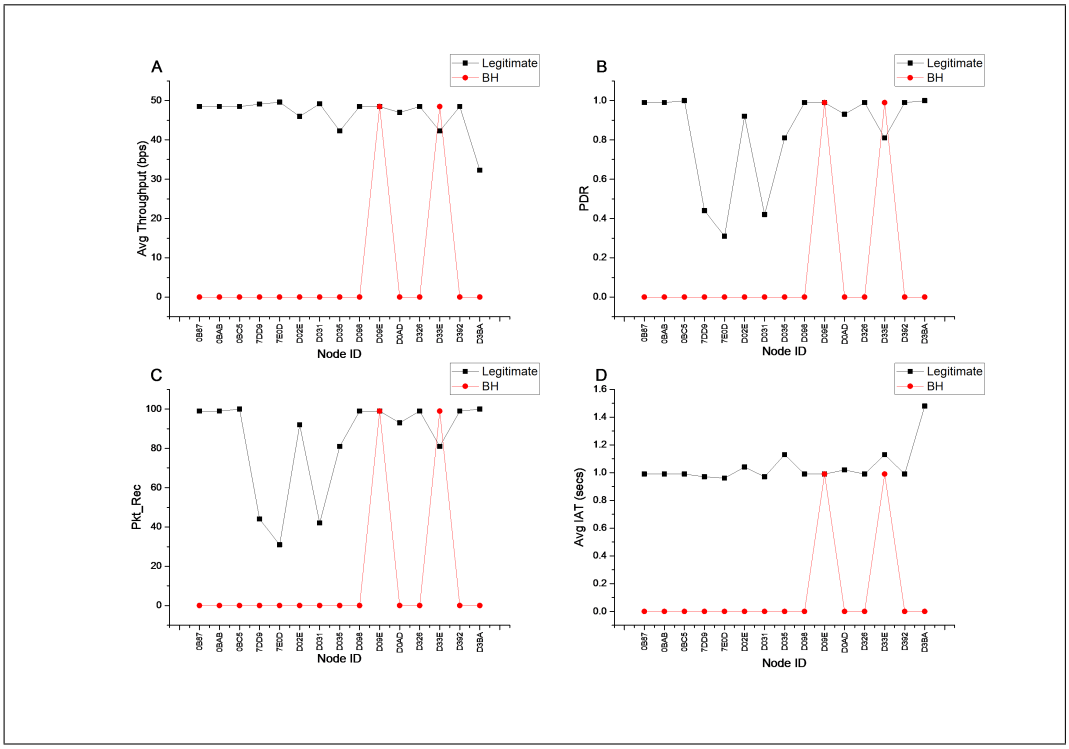

Fig. 3. Impact Analysis-Black Hole Attack

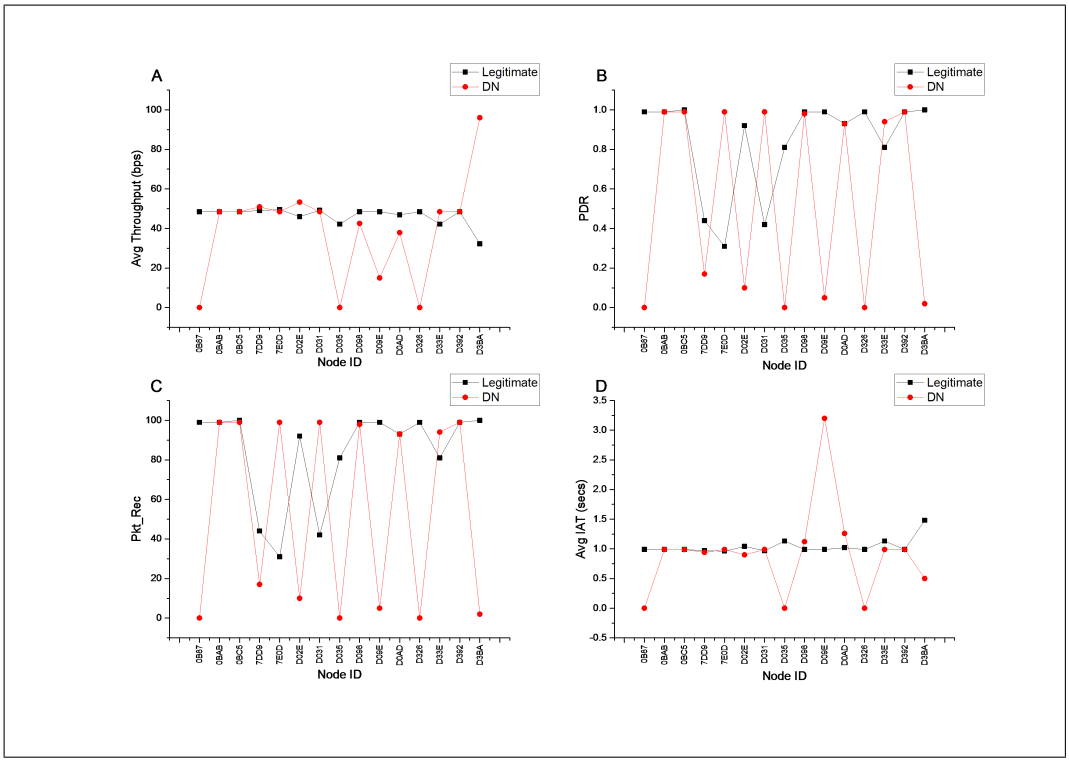

Fig. 4. Impact Analysis-Dropping Node Attack

packet received count. Fig. 8(D) shows the increased average IAT for such sensor nodes.

7) Sink Hole Attack Analysis: Like a Gray hole attacker, the Sink hole attacker also drops the data packets selectively. Besides, it influences more number of sensor nodes in the

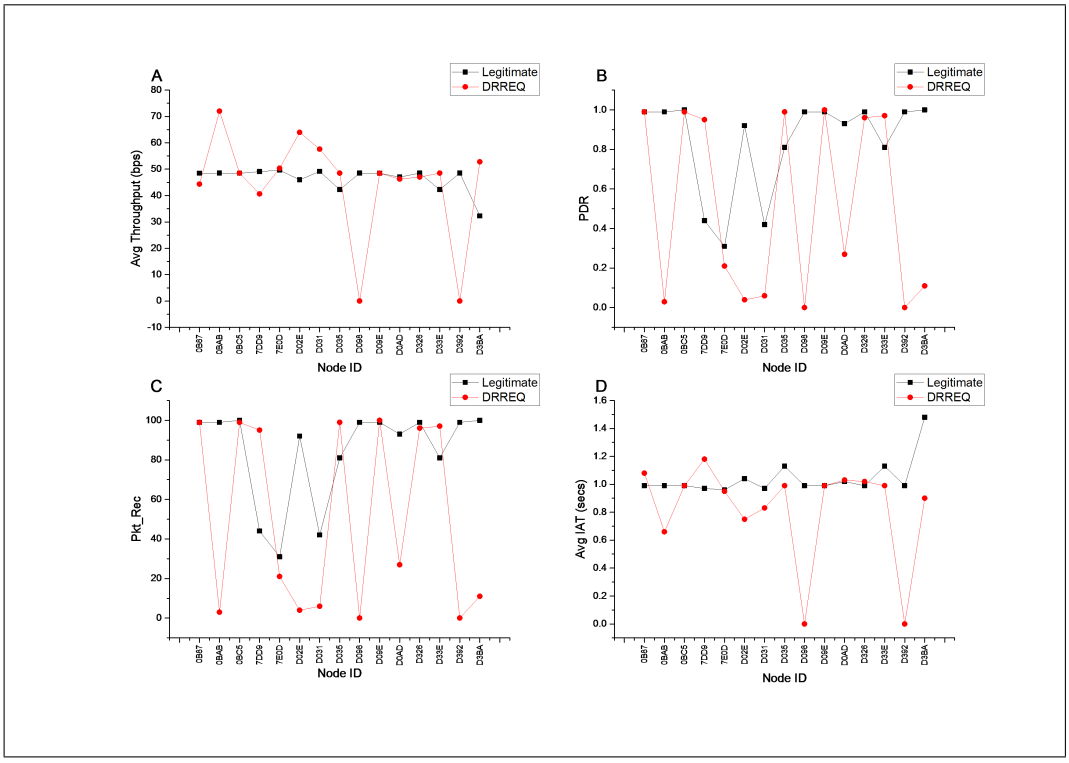

Fig. 5. Impact Analysis-Drop RREQ Attack

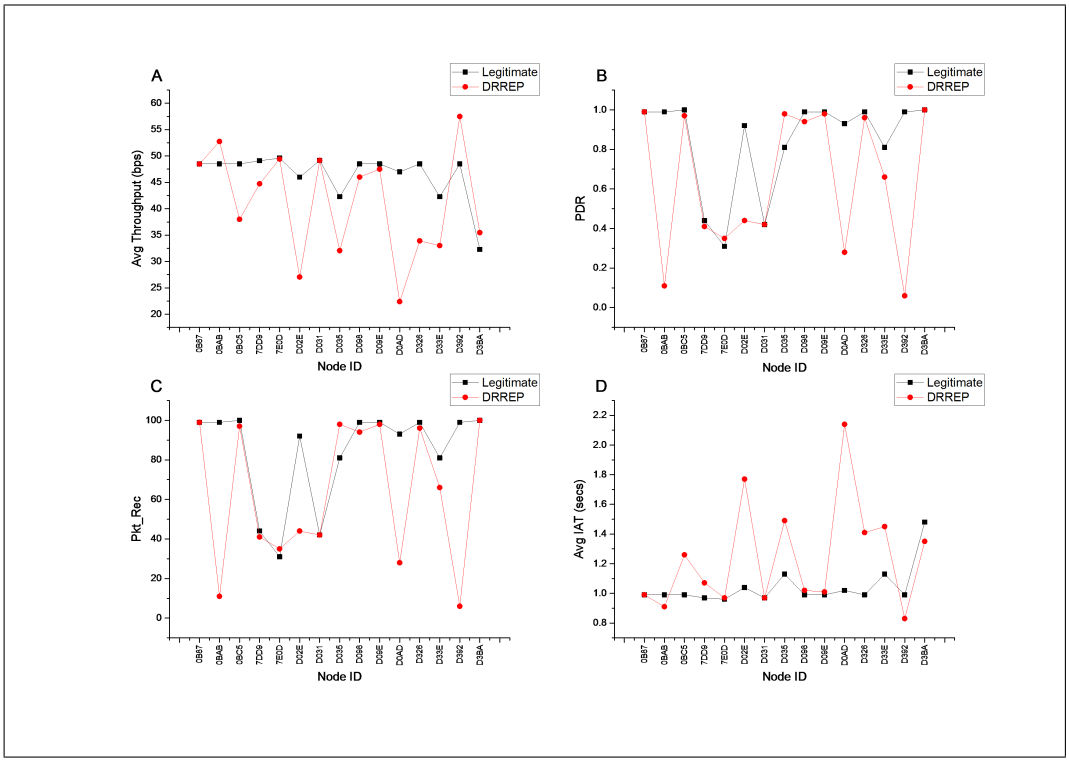

Fig. 6. Impact Analysis-Drop RREP Attack

network because it forces the sensor nodes to form their routes to the base station through it. The impact of the Sink hole attack is clearly visible in Fig. 9 as the average throughput, PDR and packet received count are decreased and the average IAT of the affected sensor nodes is increased.

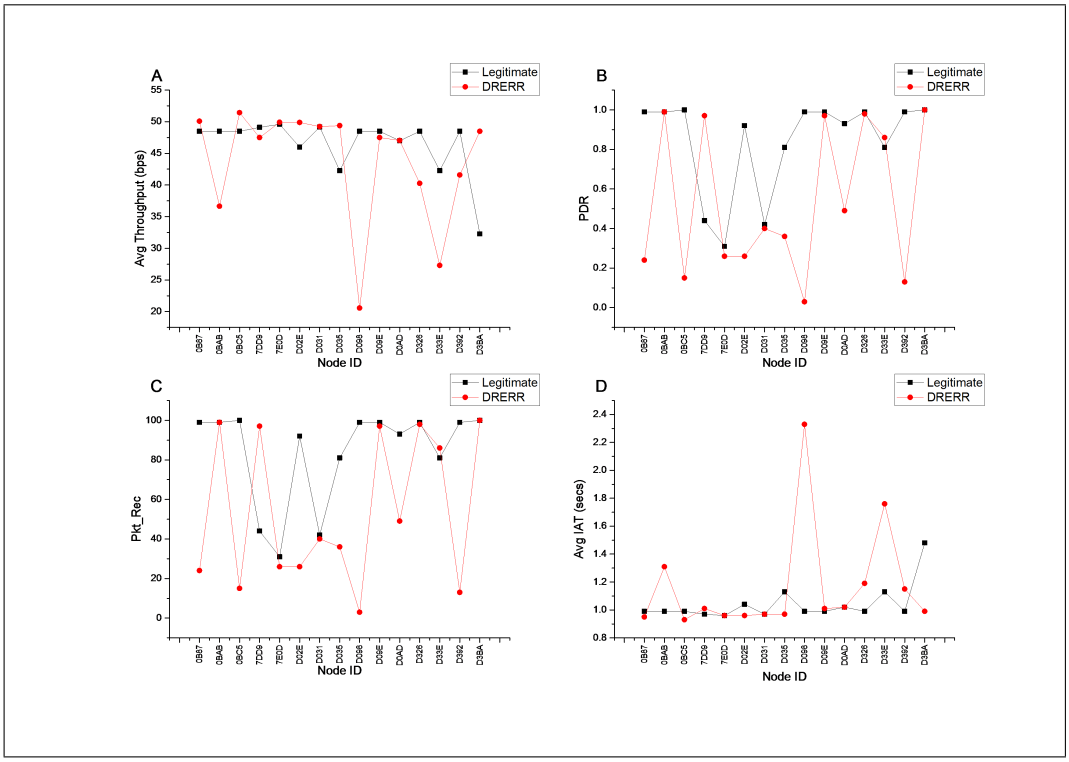

Fig. 7. Impact Analysis-Drop RERR Attack

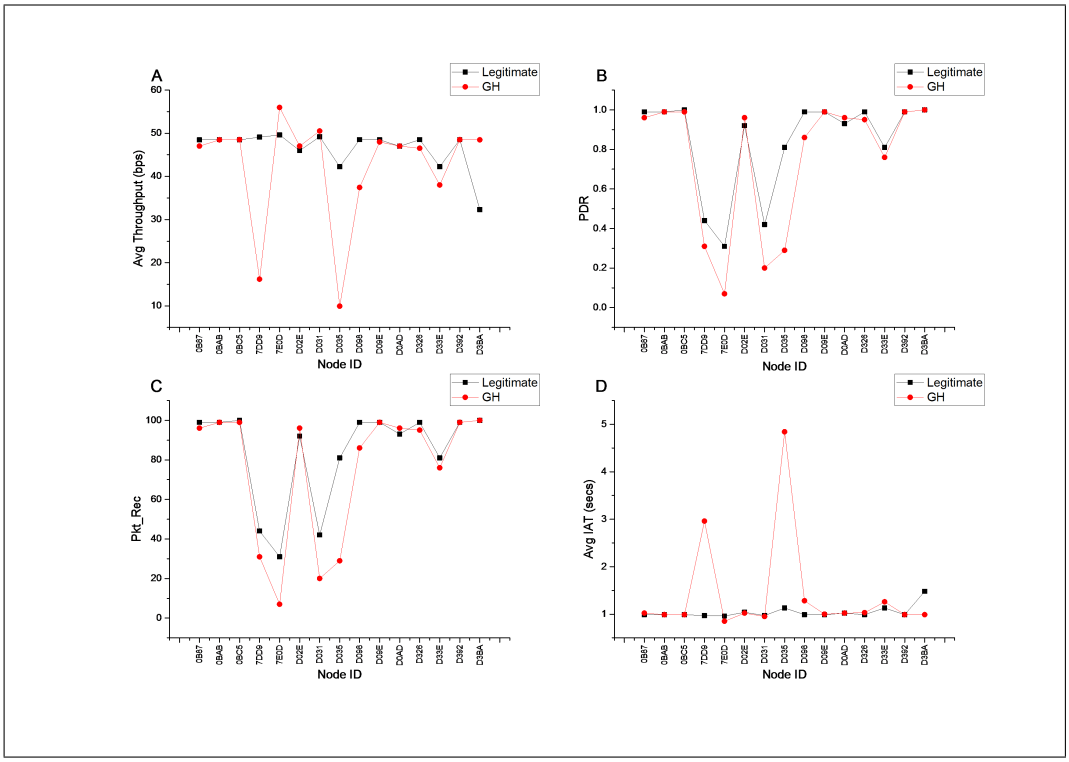

Fig. 8. Impact Analysis-Gray Hole Attack

V. Conclusion

The study presents the implementation of seven network layer attacks on a single testbed. The attacks are chosen to understand the difference between their implications on the network. The attacks are launched one at a time so that the impact can be clearly shown in terms of performance metrics.

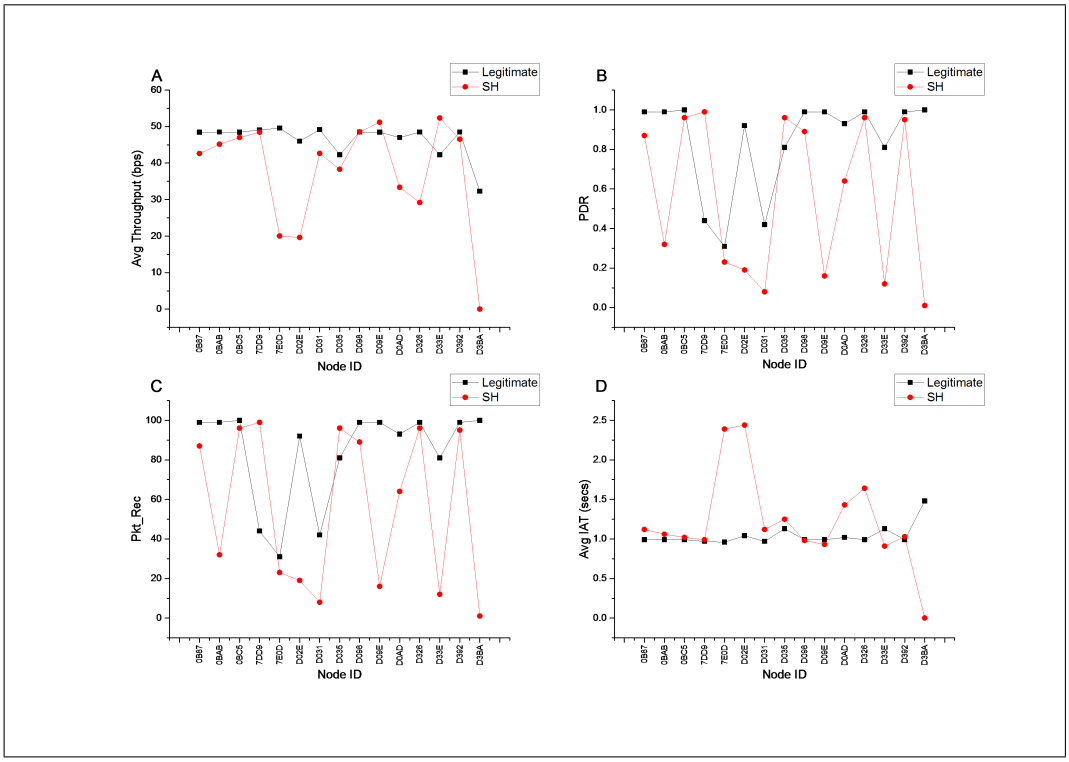

Fig. 9. Impact Analysis-Sink Hole Attack

The experiments are created to capture the network performance with and without attack. The results clearly show the impact of each attack in the testbed in terms of performance metrics. In case of an attack, the average throughput is either zero when a node could not send any data to the base station or it is reduced significantly due to selective packet drop and delayed route establishment. A similar impact is found on the PDR and the number of packets received at the base station. The average inter-arrival packet time increased in case of selective forwarding attacks. Therefore, the results depict that the impact of each attack type is visible in the testbed as per the attack definitions, in terms of network performance metrics, which validates the accurate implementation of all network layer attacks. A clear understanding of this behavior is helpful for the research community to differentiate between legitimate and attacked network.

For the future work, this experimentation is used to construct a real-time dataset for the WSN, which will further be used to propose and validate attack detection techniques in these networks.

ACKNOWLEDGMENT

The authors gratefully acknowledge the Department of Science & Technology (DST), New Delhi, India, to support financially this research under Women Scientist Scheme (WOS-A) with Grant Ref. No. SR/ WOS-A/ ET-1067/2014. The authors are highly grateful to the Department of RIC, IK Gujral Punjab Technical University, Kapurthala, Punjab, India, for providing the opportunity to conduct this investigation. The authors would also like to acknowledge, Department of CSE, Shaheed Bhagat Singh State Technical Campus (SBSSTC), Ferozepur, Punjab (India), for providing infrastructure facilities for implementing of this work.

REFERENCES

[1] P. Rawat, K. D. Singh, H. Chaouchi, and J. M. Bonnin, "Wireless sensor networks: A survey on recent developments and potential synergies," *The Journal of supercomputing*, vol. 68, no. 1, pp. 1–48, 2014.

[2] M. Tripathi, M. S. Gaur, and V. Laxmi, "Comparing the impact of black hole and gray hole attack on leach in wsn," *Procedia Computer Science*, vol. 19, pp. 1101–1107, 2013.

[3] G. Dini and M. Tiloca, "On simulative analysis of attack impact in wireless sensor networks," in *IEEE 18th Conference on Emerging Technologies & Factory Automation (ETFA)*. IEEE, 2013, pp. 1–8.

[4] M. Riecker, D. Thies, and M. Hollick, "Measuring the impact of denial-of-service attacks on wireless sensor networks," in *39th annual IEEE conference on Local Computer Networks*. IEEE, 2014, pp. 296–304.

[5] S. Chaudhary and P. Thanvi, "Performance analysis of modified aodv protocol in context of denial of service (dos) attack in wireless sensor networks," *International Journal of Engineering Research and General Science*, vol. 3, no. 3, pp. 486–491, 2015. [Online]. Available: http://pnrsolution.org/Datacenter/Vol3/Issue3/65.pdf

[6] I. Almomani and B. Al-Kasasbeh, "Performance analysis of leach protocol under denial of service attacks," in *6th International Conference on Information and Communication Systems (ICICS)*. IEEE, 2015, pp. 292–297.

[7] R. Das, S. Bal, S. Das, M. K. Sarkar, D. Majumder, A. Chakraborty, and K. Majumder, "Performance analysis of various attacks under aodv in wsn & manet using opnet 14.5," in *2016 IEEE 7th Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON)*. IEEE, 2016, pp. 1–9.

[8] C. Ioannou and V. Vassiliou, "The impact of network layer attacks in wireless sensor networks," in *International Workshop on Secure Internet of Things (SIoT)*. IEEE, 2016, pp. 20–28.

[9] A. Diaz and P. Sanchez, "Simulation of attacks for security in wireless sensor network," *Sensors*, vol. 16, no. 11, p. 1932, 2016.

[10] J. Govindasamy and S. Punniakody, "A comparative study of reactive, proactive and hybrid routing protocol in wireless sensor network under wormhole attack," *Journal of Electrical Systems and Information Technology*, vol. 5, no. 3, pp. 735–744, 2018.

[11] I. Tomic and J. A. McCann, "A survey of potential security issues in existing wireless sensor network protocols," *IEEE Internet of Things Journal*, vol. 4, no. 6, pp. 1910–1923, 2017.

[12] R. Baskar, P. Raja, C. Joseph, and M. Reji, "Sinkhole attack in wireless sensor networks-performance analysis and detection methods," *Indian Journal of Science and Technology*, vol. 10, no. 12, 2017.

[13] R. Rana and R. Kumar, "Performance analysis of aodv in presence of malicious node," *Acta Electronica Malaysia (AEM)*, vol. 3, no. 1, pp. 1–5, 2019.

[14] J. R. Gomez, H. F. V. Montoya, and A. L. Henao, "Implementing a wormhole attack on wireless sensor networks with xbee s2c devices," *Revista Colombiana de Computacion*, vol. 20, no. 1, pp. 41–58, 2019.

[15] W. C. Craig, "Zigbee: Wireless control that simply works," *Zigbee Alliance ZigBee Alliance*, 2004. [Online]. Available: https://eclass.uop.gr/modules/document/file.php/TST220/bibliography/Zigbee-tutorialZMDAmerica.pdf

[16] C. Perkins, E. Belding-Royer, and S. Das, "Rfc3561: Ad hoc on-demand distance vector (aodv) routing," 2003. [Online]. Available: https://dl.acm.org/doi/pdf/10.17487/RFC3561

[17] N. Sidhu and M. Sachdeva, "A comprehensive study of routing layer intrusions in zigbee based wireless sensor networks," *International Journal of Advanced Science and Technology*, vol. 29, no. 3, pp. 514–524, 2020. [Online]. Available: http://sersc.org/journals/index.php/IJAST/article/view/3951

[18] H. Ehsan and F. A. Khan, "Malicious aodv: Implementation and analysis of routing attacks in manets," in *11th International Conference on Trust, Security and Privacy in Computing and Communications*. IEEE, 2012, pp. 1181–1187.

[19] A. A. Korba, S. Ghanemi, and M. Nafaa, "Analysis of security attacks in aodv," in *International Conference on Multimedia Computing and Systems (ICMCS)*. IEEE, 2014, pp. 752–756.

[20] H. Moudni, M. Er-rouidi, H. Mouncif, and B. El Hadadi, "Performance analysis of aodv routing protocol in manet under the influence of routing attacks," in *International Conference on Electrical and Information Technologies (ICEIT)*. IEEE, 2016, pp. 536–542.