

Identifying sinkhole Attack in WSN'S Using Secure AODV

Sana Tak^{1*}, Ashish Trivedi²

¹Bhilai Institute of technology, Raipur (Assistant Professor, C.S.V.T.U)

²SSIPMT, Raipur (Assistant Professor, C.S.V.T.U)

¹sana.tak@bitraipur.ac.in, ²a.trivedi@ssipmt.com

ABSTRACT

Sinkhole attack is one of the most severe wireless ad hoc network assaults. A compromised or malicious node advertises incorrect routing information to present itself as a particular node and receives all network traffic in a sinkhole attack. It modifies the hidden information, such as changes made to data packets, or removes them after receiving the entire network traffic to make the network more complicated. A malicious node attempts to collect protected data from all of its neighbors. Sinkhole attacks use vulnerabilities like maximizing the sequence number or decreasing the hop count to affect the efficiency of Ad hoc networks protocols like AODV [4]. As a result, the path provided by the malicious node tends to be the best available communication path for the nodes. Sinkhole attack modifies sequence no in RREQ in DSR protocol.

Keywords

Wireless sensor network, Ad-hoc Network, AODV

Introduction

Network simulators are tools that help predict the behavior of a computer network by simulating discrete events in a network. Links, switches, hubs, applications, and so on are common components of simulated networks. The simulation model is then run to analyze the results. The simulator can then be customized to the needs of the administrators. Now a days, WLAN, UDP, TCP, IP, WAN, and other popular protocols and networks are currently in use, are usually supported by network simulators.

Configuring state elements such as connections, switches, hubs, terminals, and so on, as well as events such as packet drop rate, distribution status, and so on, are all part of the network simulation process. The trace files are the most significant performance of the simulations. Every packet and event that occurred during the simulation is recorded and evaluated using trace files. Other resources that network simulators may provide illustration analysis of patterns & possible hitch spots. The bulk of the execution is conducted in isolated duration of intervals, with occurrences in the row being implemented one by one.

Since execution is a challenging process, we can't promise that all simulators will work & will produce precise or reliable outcomes for all types of data. Network simulators include ns, NCTUNS, NetSim, and others. [3]

NS2 refers to a category of discrete occurrence network simulators that includes NS-I/II & NS-III. They're all discrete-event network simulators, which are widely preferred in investigation &

education. NS-II is open-source software that is freely accessible for study, development, and use under the GNU GPLv2 license. [3]

Methodology

■ Parameters Description

Total five parameters are considered in the research work, which are:

- i. Packet Delivery Ratio (PDR)
- ii. End-to-End Delay (E-2-E Delay)
- iii. Average Throughput
- iv. Normalized Routing Load (NRL)
- v. Routing Overhead (RO)

i. Packet Delivery Ratio (PDR)

The packet distribution ratio is a vital metric for assessing the efficiency of any protocol relevant to routing in a network. The protocol's output is determined by the simulation parameters chosen. The size of the packet, range of transmission, no. of nodes & network configuration are the most important parameters. [2] The overall count of information packets arriving at sink nodes divided by the total number of information packets transmitted from source nodes yields the PDR. To put it another way, the packet distribution ratio is the proportion of packets retrieved at the sink location to packets transmitted from the source location. When the packet delivery ratio is high, the output is better. It can be interpreted mathematically as an equation. (i).

$$PDR = \frac{TOTAL\ PACKETS\ RECIEVED\ BY\ DESTINATION\ NODES}{OTAL\ PACKETS\ SENT\ BY\ SENDER\ NODES} \times 100 \quad (i)$$

ii. End-to-End Delay (E-2-E Delay)

Typically, the duration it acquires for a data to transmit from its source location to its sink location across the network is known as end-to-end latency. The average of it could be determined via taking the average of all successfully delivered messages' end-to-end delays. As a result, the packet delivery ratio has an effect on end-to-end delay. Packet loss becomes more likely as the distance existing between the source node & sink node grows. The typical end-to-end delay takes into account all network delays, such as buffering path discovery latency, MAC retransmission delays, and transmission/propagation delays [11-14]. The same can be interpreted mathematically in form of an equation. (ii).

$$\text{Avg E-2-E Delay} = \sum_{i=1}^n (Tr - Ts) \quad (ii)$$

Tr= Time of Reception, Ts= Time of Transmission, n = No. of successfully delivered packets

iii. Average Throughput

It's the total throughput's average. It's also counted in packets per TIL unit. Time Interval Length (TIL) can be represented mathematically as an equation. (iii).

$$\text{Average Throughput} = \frac{\text{Received packet size}}{(\text{stoptime} - \text{starttime})} \times \left(\frac{8}{1000}\right) \quad (iii)$$

iv. Normalized Routing Load (NRL)

In a simulation, this is the ratio of routing-related broadcastings (RREQ, RREP, RERR, and so on) to data transmissions. A transmission occurs when one node sends or forwards a packet. The routing load per unit data was fully transmitted to the destination in either case [5,9,10]. It can be represented mathematically as an equation (iv).

$$\text{NRL} = \frac{\text{No. of RREQ} + \text{RREP} + \text{RERR} + \text{RREQ}}{\text{No. of packets successfully delivered}} \quad (iv)$$

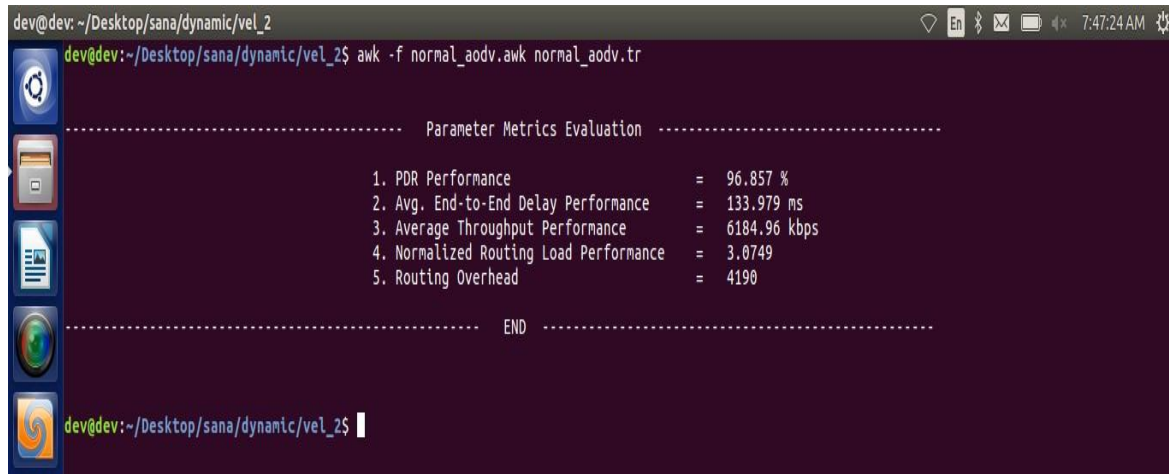
v. Routing Overhead (RO)

During the simulation, it is the total number of control or routing (RTR) packets created by the routing protocol. Routing overhead is calculated for all packets sent or forwarded at the network layer.

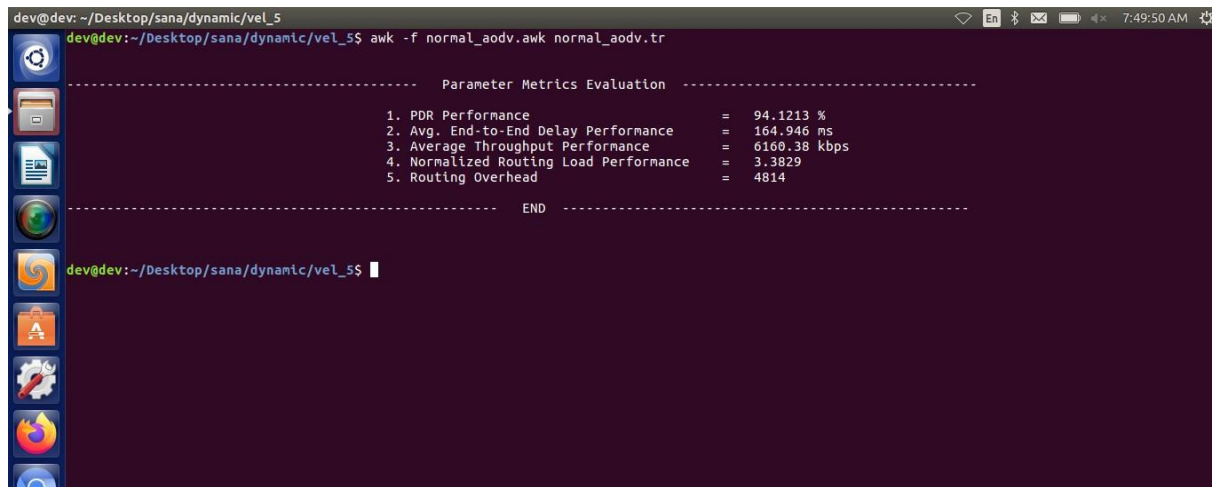
3. Terminal outputs Snapshots

As it is discussed that there is total three set of scenarios prepared i.e. normal scenario, sinkhole scenario and secure scenario, so different outputs are achieved.

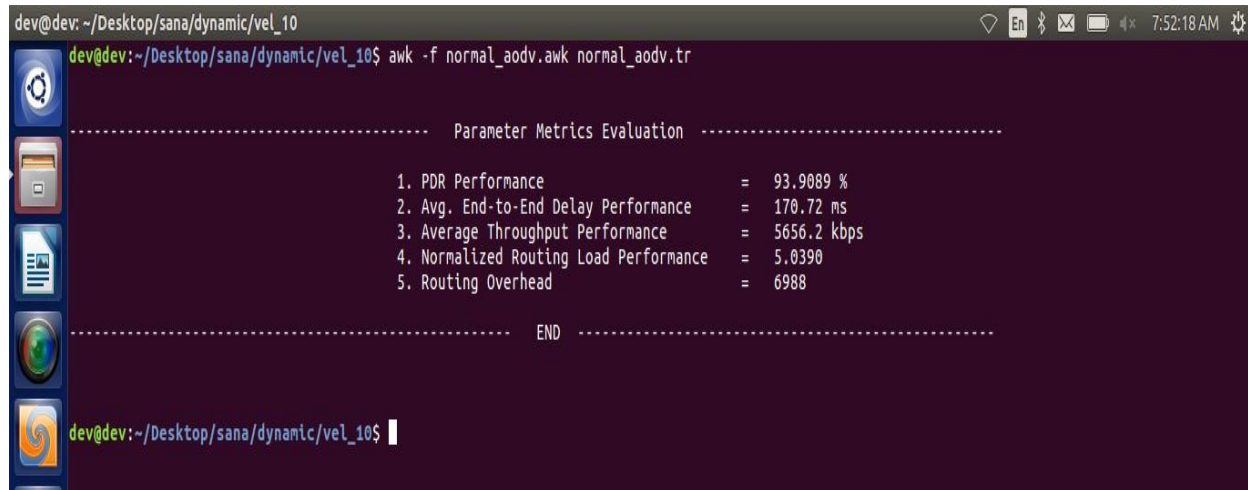
SET 1 : Output Result For Normal AODV Scenario



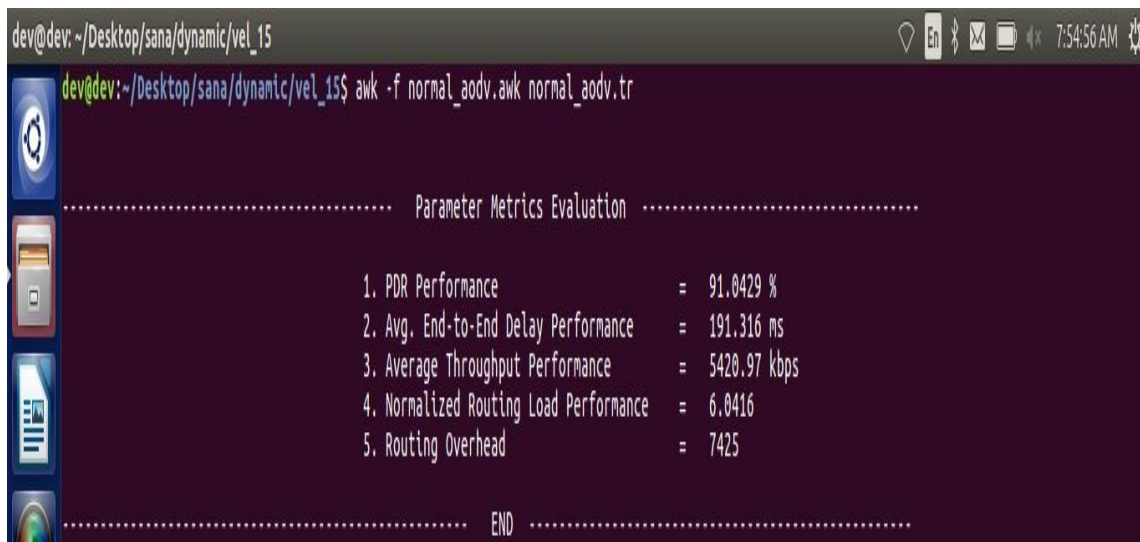
Result For Normal AODV Scenario for velocity of nodes 2 m/s
Figure 1



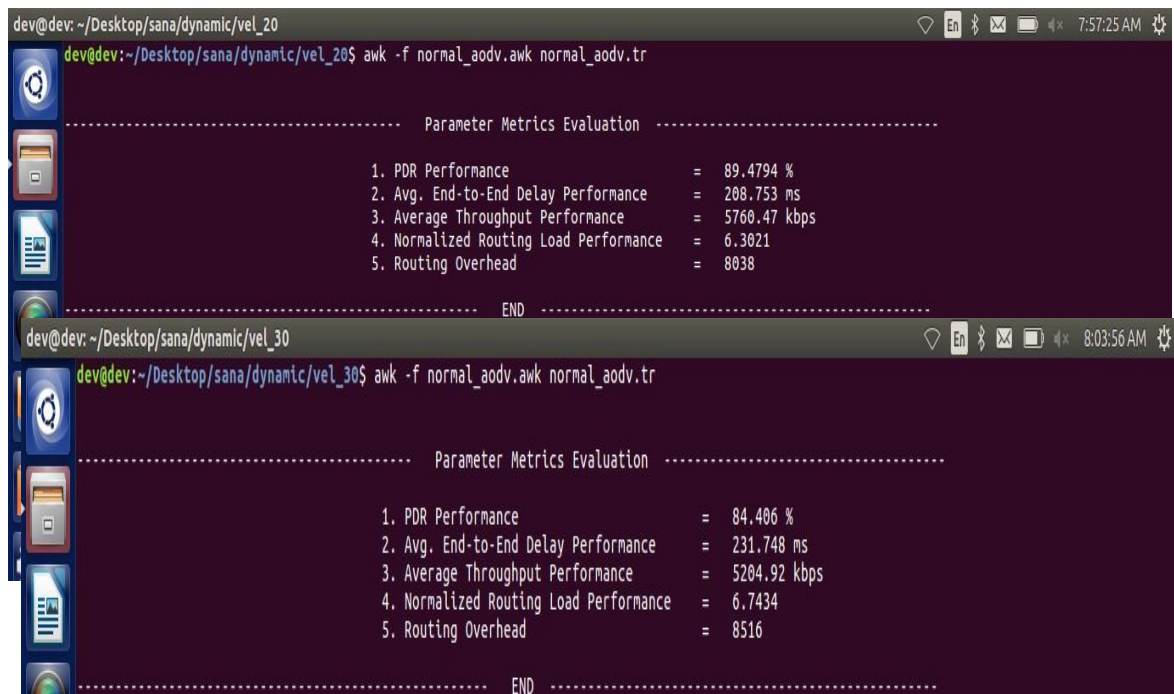
Result For Normal AODV Scenario for velocity of nodes 5 m/s
Figure 2



Result For Normal AODV Scenario for velocity of nodes 10 m/s
Figure 3



Result For Normal AODV Scenario for velocity of nodes 15 m/s
Figure 4



Result For Normal AODV Scenario for velocity of nodes 20 m/s

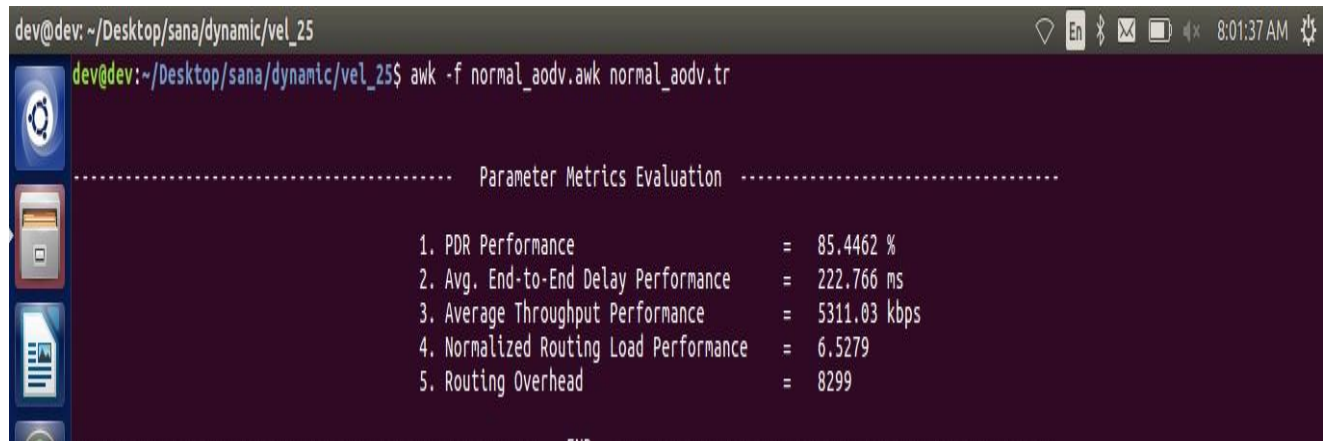


Figure 5

Result For Normal AODV Scenario for velocity of nodes 25 m/s

Figure 6

Result For Normal AODV Scenario for velocity of nodes 30 m/s Figure 7

SET 2 : Output Result For Sinkhole AODV Scenario

```
dev@dev: ~/Desktop/sana/dynamic/vel_2
dev@dev:~/Desktop/sana/dynamic/vel_2$ awk -f sinkhole_aodv.awk sinkhole_aodv.tr

----- Parameter Metrics Evaluation -----

1. PDR Performance           = 76.4818 %
2. Avg. End-to-End Delay Performance = 158.673 ms
3. Average Throughput Performance = 3752.06 kbps
4. Normalized Routing Load Performance = 3.7978
5. Routing Overhead         = 5082

----- END -----
```

Result For Sinkhole AODV Scenario for velocity of nodes 2 m/s Figure 8

```
dev@dev: ~/Desktop/sana/dynamic/vel_5
dev@dev:~/Desktop/sana/dynamic/vel_5$ awk -f sinkhole_aodv.awk sinkhole_aodv.tr

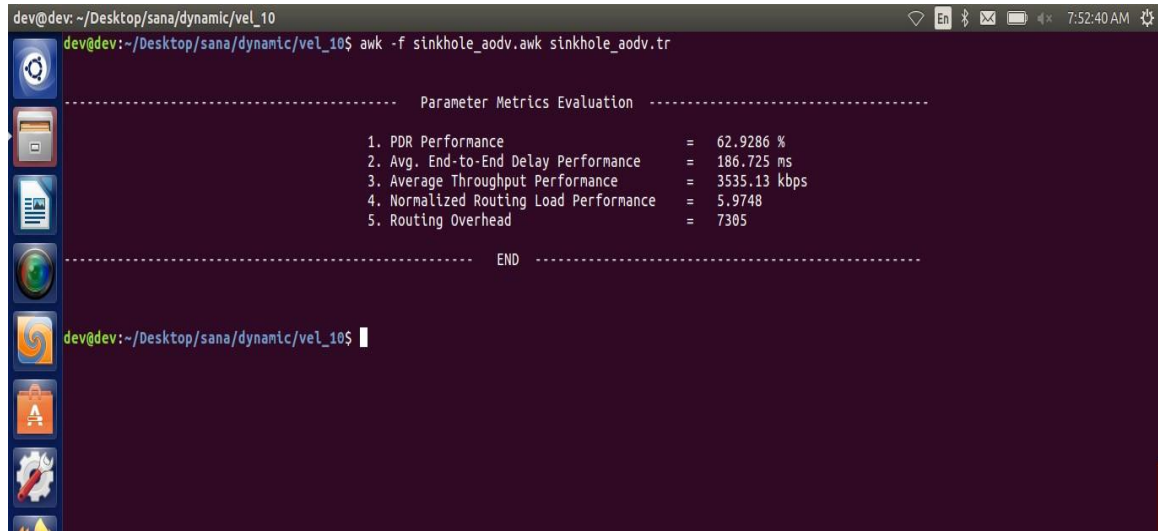
----- Parameter Metrics Evaluation -----

1. PDR Performance           = 67.9226 %
2. Avg. End-to-End Delay Performance = 179.289 ms
3. Average Throughput Performance = 3623.76 kbps
4. Normalized Routing Load Performance = 4.0112
5. Routing Overhead         = 5743

----- END -----

dev@dev:~/Desktop/sana/dynamic/vel_5$
```

Result For Sinkhole AODV Scenario for velocity of nodes 5 m/s Figure 9



A terminal window titled 'dev@dev: ~/Desktop/sana/dynamic/vel_10' showing the execution of an awk script 'sinkhole_aodv.awk' on a file 'sinkhole_aodv.tr'. The output displays five performance metrics for a Sinkhole AODV scenario at 5 m/s velocity. The metrics are: 1. PDR Performance (62.9286 %), 2. Avg. End-to-End Delay Performance (186.725 ms), 3. Average Throughput Performance (3535.13 kbps), 4. Normalized Routing Load Performance (5.9748), and 5. Routing Overhead (7305). The terminal also shows the command prompt and the file path.

```
dev@dev: ~/Desktop/sana/dynamic/vel_10$ awk -f sinkhole_aodv.awk sinkhole_aodv.tr
```

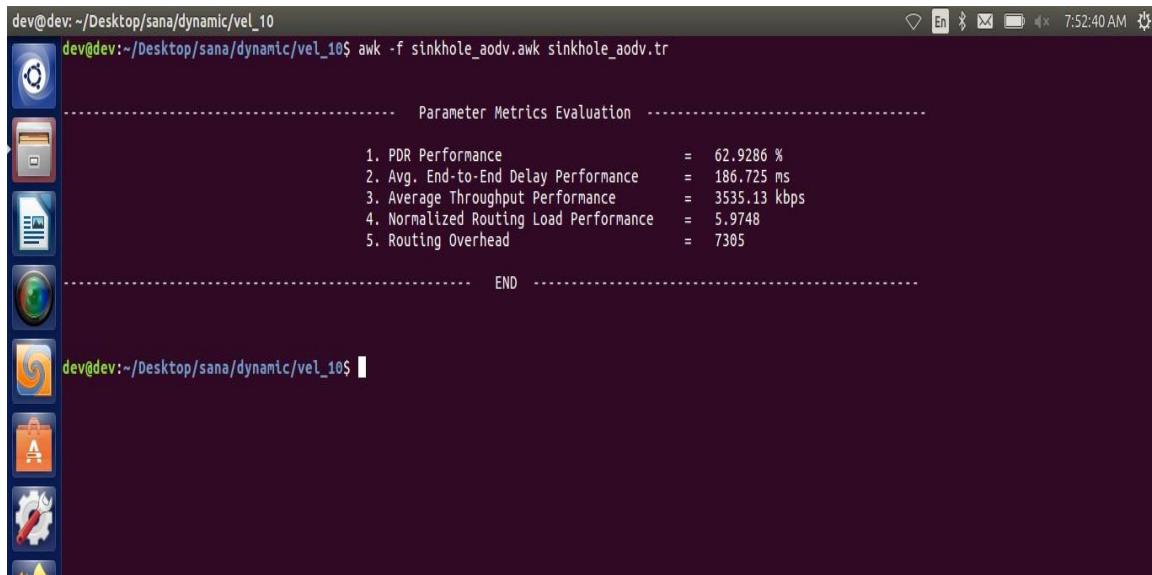
```
----- Parameter Metrics Evaluation -----
```

1. PDR Performance	=	62.9286 %
2. Avg. End-to-End Delay Performance	=	186.725 ms
3. Average Throughput Performance	=	3535.13 kbps
4. Normalized Routing Load Performance	=	5.9748
5. Routing Overhead	=	7305

```
----- END -----
```

```
dev@dev:~/Desktop/sana/dynamic/vel_10$
```

Result For Sinkhole AODV Scenario for velocity of nodes 10 m/s Figure 10



A terminal window titled 'dev@dev: ~/Desktop/sana/dynamic/vel_10' showing the execution of an awk script 'sinkhole_aodv.awk' on a file 'sinkhole_aodv.tr'. The output displays five performance metrics for a Sinkhole AODV scenario at 10 m/s velocity. The metrics are: 1. PDR Performance (62.9286 %), 2. Avg. End-to-End Delay Performance (186.725 ms), 3. Average Throughput Performance (3535.13 kbps), 4. Normalized Routing Load Performance (5.9748), and 5. Routing Overhead (7305). The terminal also shows the command prompt and the file path.

```
dev@dev: ~/Desktop/sana/dynamic/vel_10$ awk -f sinkhole_aodv.awk sinkhole_aodv.tr
```

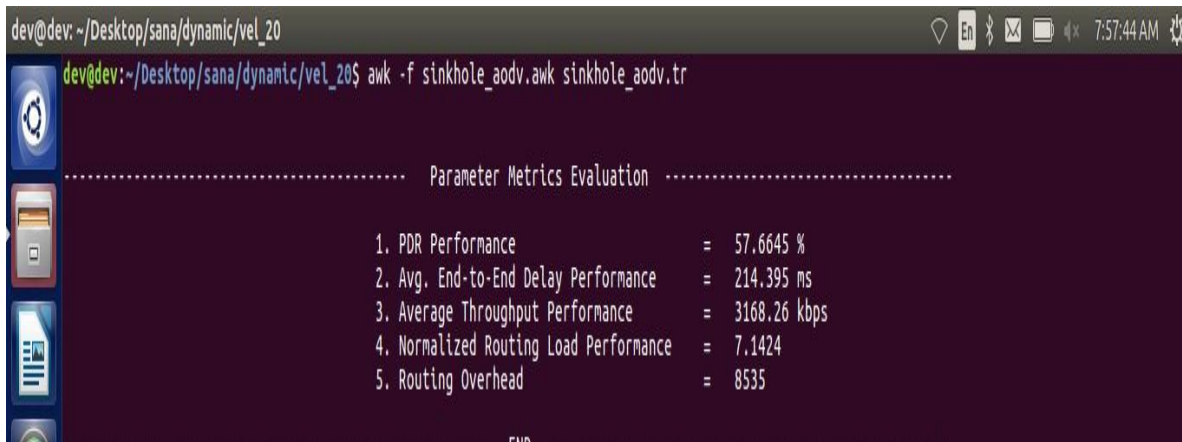
```
----- Parameter Metrics Evaluation -----
```

1. PDR Performance	=	62.9286 %
2. Avg. End-to-End Delay Performance	=	186.725 ms
3. Average Throughput Performance	=	3535.13 kbps
4. Normalized Routing Load Performance	=	5.9748
5. Routing Overhead	=	7305

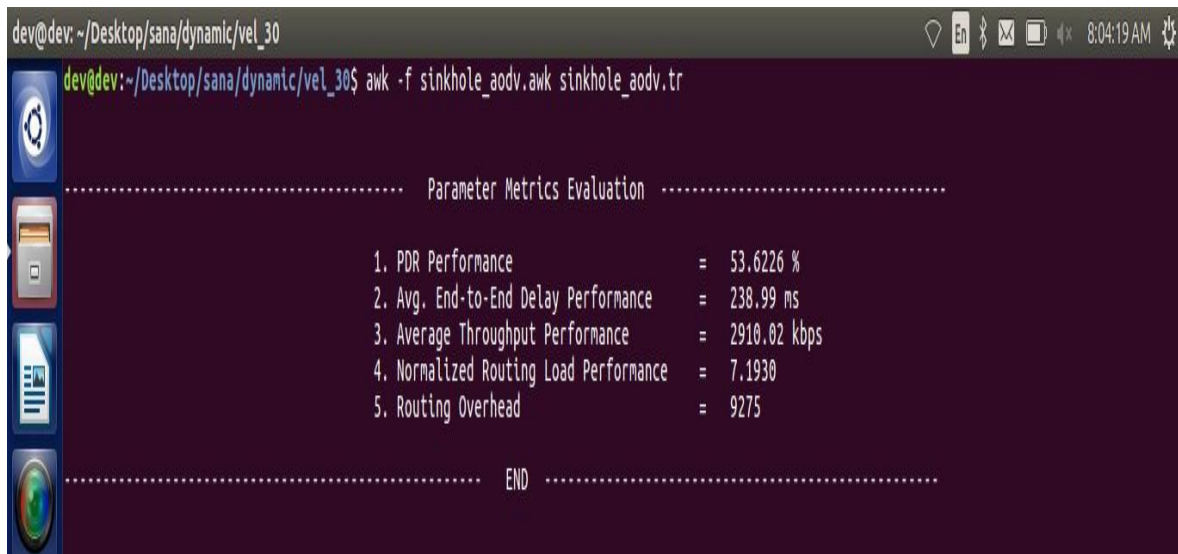
```
----- END -----
```

```
dev@dev:~/Desktop/sana/dynamic/vel_10$
```


Result For Sinkhole AODV Scenario for velocity of nodes 15 m/s
Figure 11



Result For Sinkhole AODV Scenario for velocity of nodes 20 m/s
Figure 12



Result For Sinkhole AODV Scenario for velocity of nodes 30 m/s
Figure 13

SET 3 : Output Result for Secure AODV Scenario

```
dev@dev: ~/Desktop/sana/dynamic/vel_2
dev@dev: ~/Desktop/sana/dynamic/vel_10
dev@dev: ~/Desktop/sana/dynamic/vel_10$ awk -f secure_aodv.awk secure_aodv.tr

----- Parameter Metrics Evaluation -----

1. PDR Performance           = 71.6418 %
2. Avg. End-to-End Delay Performance = 142.267 ms
3. Average Throughput Performance = 4147.88 kbps
4. Normalized Routing Load Performance = 4.6471
5. Routing Overhead         = 6543

----- END -----
----- FIN -----
```

Result For Secure AODV Scenario for velocity of nodes 2 m/s
Figure 14

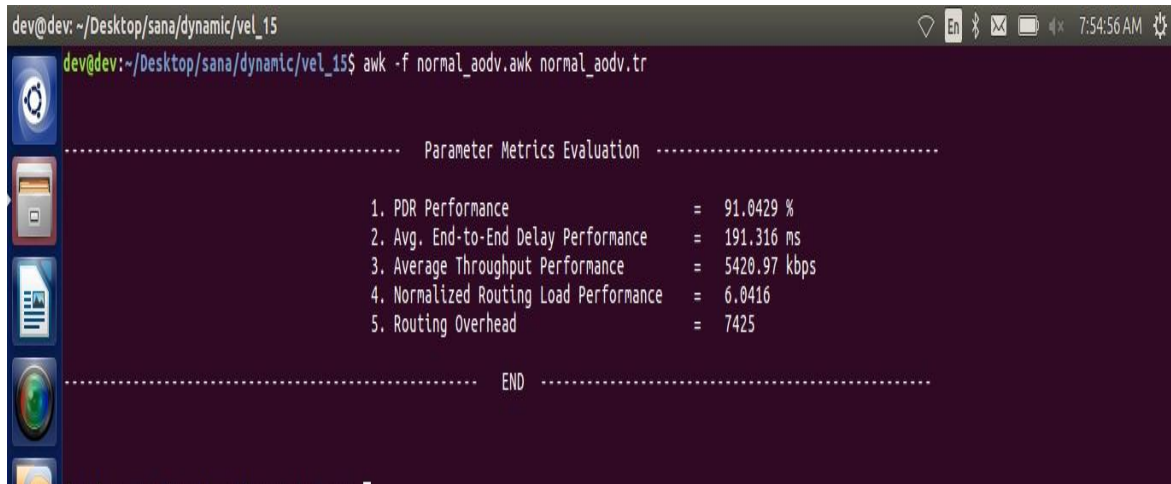
```
dev@dev: ~/Desktop/sana/dynamic/vel_5
dev@dev: ~/Desktop/sana/dynamic/vel_5$ awk -f normal_aodv.awk normal_aodv.tr

----- Parameter Metrics Evaluation -----

1. PDR Performance           = 94.1213 %
2. Avg. End-to-End Delay Performance = 164.946 ms
3. Average Throughput Performance = 6160.38 kbps
4. Normalized Routing Load Performance = 3.3829
5. Routing Overhead         = 4814

----- END -----
```

Result For Secure AODV Scenario for velocity of nodes 5 m/s
Figure 15



Result For Secure AODV Scenario for velocity of nodes 10 m/s
Figure 16

Result For Secure AODV Scenario for velocity of nodes 15 m/s
Figure 17for velocity of nodes = 20 m/s



Result For Secure AODV Scenario for velocity of nodes 20 m/s
Figure 18

```
dev@dev: ~/Desktop/sana/dynamic/vel_25
dev@dev:~/Desktop/sana/dynamic/vel_25$ awk -f normal_aodv.awk normal_aodv.tr

----- Parameter Metrics Evaluation -----

1. PDR Performance           = 85.4462 %
2. Avg. End-to-End Delay Performance = 222.766 ms
3. Average Throughput Performance = 5311.03 kbps
4. Normalized Routing Load Performance = 6.5279
5. Routing Overhead         = 8299

----- END -----
```

Result For Secure AODV Scenario for velocity of nodes 25 m/s
Figure 19

```
dev@dev: ~/Desktop/sana/dynamic/vel_30
dev@dev:~/Desktop/sana/dynamic/vel_30$ awk -f normal_aodv.awk normal_aodv.tr

----- Parameter Metrics Evaluation -----

1. PDR Performance           = 84.406 %
2. Avg. End-to-End Delay Performance = 231.748 ms
3. Average Throughput Performance = 5204.92 kbps
4. Normalized Routing Load Performance = 6.7434
5. Routing Overhead         = 8516

----- END -----
```

Result For Secure AODV Scenario for velocity of nodes 30 m/s
Figure 20

The Below Mentioned is the algorithm used for calculating the result

Algorithm [1]

1. With Finite number of mobile nodes Set MANET network
2. With the MANET Network, the network defines the source and destination nodes.
3. The source sends network RREP to create a route to the sink node.
4. The shortest path from source to destination will be determined based on hop count and sequence number.
5. In the network, the delay per hop will be determined.
6. If (delay < defined delay)
7. Evaluate the Euclidian distance between individual node.
8. Identify malicious nodes in the network and isolate them using hop count tracking and RSSI-based schemes.
9. Else
10. Continuation of the source from the source to the destination.

Results

The following chart shows the results:

Formula used for calculating :

$$\% \text{ of Improvement} = \frac{\sum(\text{Old value} - \text{new value})}{\sum(\text{old value})} * 100$$

Parameter	Sinkhole_AODV	Secure_AODV	% of Improvement
PDR	62.11	70.53	13.56
E-2-E Delay	201.04	159.31	20.75
Throughput	3335.36	3719.34	11.51
NRL	6.05	4.97	17.85
RO	7626	6561	13.96

Result Showing the Percentage Of Improvement Based On Various Parameters
Table 1

Discussions

Total five parameters are considered in the research work, which are:

- i. Packet Delivery Ratio (PDR)
- ii. End-to-End Delay (E-2-E Delay)
- iii. Average Throughput
- iv. Normalized Routing Load (NRL)
- v. Routing Overhead (RO)

Conclusion

1. Packet Distribution Ratio: This is a phenomenon in which a packet travels from a source and arrives at its destination successfully. Packet distribution would be improved until the attack is isolated from the network.
2. Throughput: The average rate at which packets are successfully transmitted over a communication channel is known as throughput. Throughput would be improved until the attack is isolated from the network.
3. Delay, NRL, and RO: These terms refer to the average time it takes data packets to reach their destination. In this technique, the attack AODV scenario's delay, NRL, and RO will be increased, while the current stable AODV scenario's delay, NRL, and RO will be reduced.

Limitations and Future Studies

For future consideration the security of the system can be an important domain of research. This proposed system is also useful in other types of attack to prevent it.

References

- [1] Manpreet Kaur, Amarvir Singh. "Detection and Mitigation of Sinkhole Attack in Wireless Sensor Network", 2016 International Conference on Micro-Electronics and Telecommunication Engineering (ICMETE), 2016
- [2] Prajakta M., Dr. Nupur. "Performance Evaluation and Statistical Analysis of MANET routing Protocols for RPGM and MG" , International Journal of Advanced Computer Science and Applications, 2013
- [3] "Intelligent Computing, Networking, and Informatics" , Springer Science and Business Media LLC, 2014
- [4] G.Keerthana, G. Padmavathi (2016), Detecting Sinkhole Attack in Wireless Sensor Network using Enhanced Particle Swarm Optimization Technique, International Journal of Security and Its Applications (IJSIA), Vol. 10, No. 3 (2016).
- [5] Anna Zakrzewska, Leszek Koszalka, Iwona Pozniak-Koszalka. "Performance Study of Routing Protocols for Wireless Mesh Networks" , 2008 19th International Conference on Systems Engineering, 2008
- [6] Daniel Dallas, Christopher Leckie, Kotagiri Ramamohanarao; Hop- Count Monitoring: Detecting Sinkhole Attacks in Wireless Sensor Networks 15th IEEE ICN, 2007, ICON 2007, pp.176-181.
- [7] Kesav Unnithan S L, Lakshmi Devi C, Sreekuttan Unnithan C (2015), Survey of Detection of Sink Hole Attack in Wireless Sensor Network, International Journal of Computer Science and Information Technologies (IJCSIT), Vol 6(6), 2015, 4904-4909.

- [8] Md. Ibrahim Abdullah, Detecting Sinkhole Attacks In Wireless Sensor Network using Hop Count, IJCNS 2015,3,50-5
- [9] Md. Khaja Mohiddin and V.B.S. Srilatha Indira Dutt, (2017). Minimization of Energy Consumption Using X-Layer Network Transformation Model for IEEE 802.15.4-Based MWSNs. Proceedings of the 5th International Conference on Frontiers in Intelligent Computing: Theory and Applications, Advances in Intelligent Systems and Computing (AISC), 515, 741-751.
- [10] Md. Khaja Mohiddin and V.B.S. Srilatha Indira Dutt, (2017). An Efficient Energy Optimization XLN Operation Model for IEEE 802.15.4-Based Mobile WSNs. International Journal of Control Theory and Applications (IJCTA), 10(9), 255-264.
- [11] Md. Khaja Mohiddin and V.B.S. Srilatha Indira Dutt, (2019). An Optimum Energy Consumption Hybrid Algorithm for XLN Strategic Design in WSNs. International Journal of Computer Networks and Communications (IJCNC), 11(4), 61-80.
- [12] Md. Khaja Mohiddin and V.B.S. Srilatha Indira Dutt, (2019). Routing Path Estimation Based on RWS Method for Competent Energy Dissipation Employing X-Layer Network. International Journal of Recent Technology and Engineering (IJRTE), 8(2), 6296-6303.
- [13] Md. Khaja Mohiddin and V.B.S. Srilatha Indira Dutt, (2019) “XLN Protocol Implementation for Efficient Outperforming of PDR parameter in WSN. International Journal of Advanced Science and Technology (IJAST), 29(5), 8836-8851.
- [14] Md. Khaja Mohiddin and V.B.S. Srilatha Indira Dutt, (2020) “Mobility Error Prediction based LAB Scheduling Algorithm for Optimizing System Throughput in Wireless Sensor Networks. International Journal on Emerging Technologies (IJET), 11(2), 1087-1092.