Volume-6, Issue-2, February - 2017 • ISSN No 2277 - 8160 IF : 3.62 | IC Value 80.26

Original Research Paper Engineering

Implementation of Master AODV using NS2 to mitigate Grayhole attack in MANET

K.Madhuri Research Scholar, Rayalaseema University Kurnool, India

N.Kasi Viswanath Professor and Head, GPREC, Kurnool, India

ABSTRACT *A Mobile Ad hoc Network (MANET) consists of mobile nodes which move independently in an open environment. Communication between the nodes in a MANET is enabled using intermediate routers. MANET has characteristics such as open medium, dynamic network topology, lack of centralized monitoring, and lack of clear defense mechanisms which makes it easy for several routing attacks to take place in a MANET. In MANET routing, intermediate nodes can act as malicious nodes which become a threat to the security. Grayhole is the common attack in ad hoc routing in which the malicious node uses the process of routing to say that it has the shortest path to the destination. Once it receives the data packets, it drops some data packets and forwards some data packets to its neighbors. The Grayhole node does not follow the prescribed communication model. Data Transmission is established between nodes using UDP agent and CBR traffic. Sender sends the data via attacker. Source node transfers data to attacker assuming that it has the shortest route to Destination. Attacker partially forwards the data packets to its neighbors and partially drops the data packets.*

KEYWORDS : Manet,Attacks, Performance metrics,prevention.

The author proposes the prevention of Grayhole attack by applying a technique called Trust Based mechanism [4] and modifying the existing AODV routing algorithm as Master AODV and simulating the performance of the Manet using Ns2.

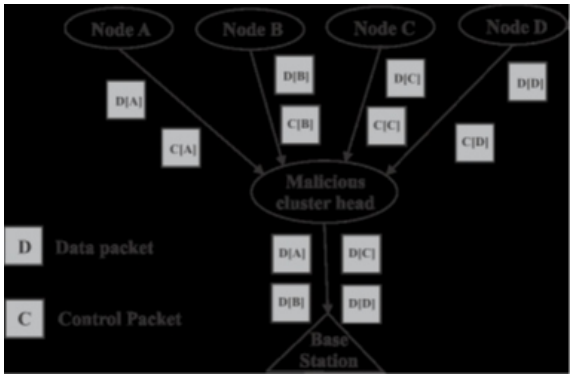


Fig 1 Trust based technique for Grayhole prevention

Every node in cluster will calculate the trust value for the cluster head. Trust value can be calculated by considering the two components of trust i.e. *social trust and QoS trust.* Social *trust* includes the parameter like intimacy, honesty, privacy etc. Whereas QoS *trust* include parameter like cooperativeness, reliability, energy consumption, task completion etc.

The detection mechanism is as follows:

The first task in the detection mechanism is to calculate the trust value for the cluster head. Therefore every node in cluster will calculate the trust value for the cluster head of its cluster.

The node monitors the behavior of the cluster head and calculates the trust value using the data collected by monitoring the behavior of the node.

The trust value calculated by each node is independent of each other. Trust value calculated by a node in cluster will not influence the trust value calculated by other node in same cluster. Trust values are calculated at two level, node level and cluster level. At node level, node calculates the trust value of cluster head for each node in cluster separately and at cluster level, it is the aggregate trust value of cluster head for the cluster. Cluster level trust value is calculated to have the aggregated view about the performance of cluster head and to use this trust value as a backup for the node level trust value. If the attack goes undetected then it can be detected at cluster level.

Proposed algorithm Master AODV algorithm is modified AODV using the Trust based technique to overcome the Grayhole attack.

The performance evaluation is done for the following performance metrics[3] and then the efficiency of the Manet is analyzed during the attack and after applying the prevention technique

1. Packet Delivery Ratio(PDR)

The ratio of the number of delivered data packets to the destination. This illustrates the level of delivered data to the destination.

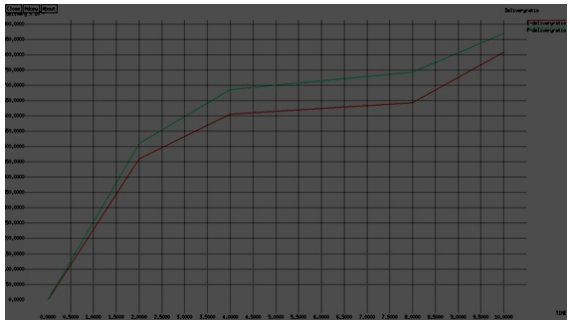
PDR = ∑number of packet received/∑ number of packets sent

Performance metrics for varying time

Table 1 PDR in the presence of malicious node(Attack) and after prevention

Time(ms)	PDR (Attack)	PDR(Prevention)
2	0.459	0.509
4	0.606	0.686
8	0.642	0.742
10	0.808	0.868

From the above table,we can conclude that the PDR after applying MasterAODV is more compared to the PDR during attack.



X-axis Time Y-axis PDR

2. Packet Drop Ratio

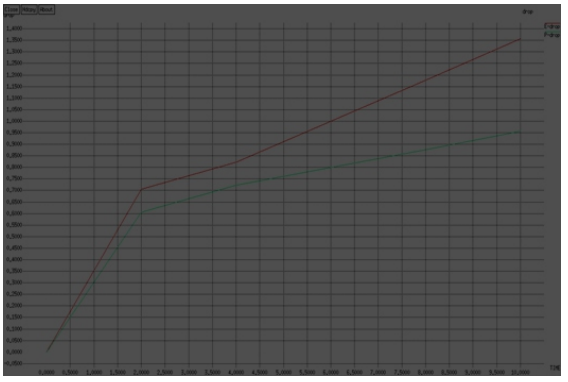
The ratio of number of packets dropped at the time of simulation. It is calculated by

Packet Drop Ratio = (Number of packets sent - Number of packets received)/100

Table 2 Packet drop ratio in the presence of malicious node(Attack) and after prevention

Time(ms)	Packet drop ratio (Attack)	Packet drop ratio(Prevention)
2	0.705	0.605
4	0.821	0.721
8	1.176	0.876
10	1.356	0.956

X-Graph for Packet drop ratio



X-axis Time Y-axis Packet drop ratio

3. Throughput

Throughput can be defined as the ratio of the packets that have been received to the simulation time.

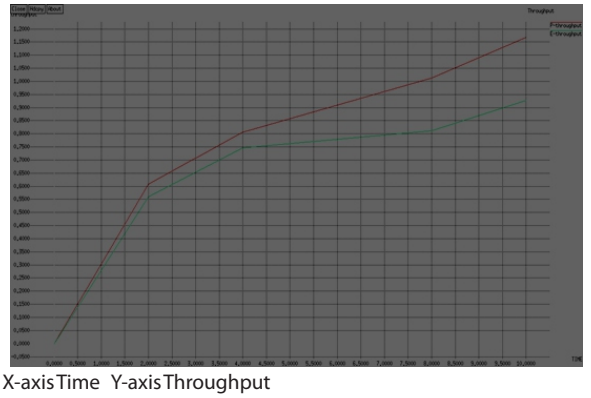
Throughput= packets received / simulation time

Table 3 Throughput in the presence of malicious nodes(Attack) and after prevention

Time(ms)	Throughput(Attack)	Throughput(Prevention)
2	0.559	0.609
4	0.746	0.806
8	0.812	1.012
10	0.926	1.166

From the above table,we can see that the Throughput has increased after applying the Master AODV.

X-Graph for Throughput



X-axis Time Y-axis Throughput

4. Average End – to – End Delay

This is the average time delay consumed by data packets to propagate from source to destination. This delay includes the total time of transmission i.e. propagation time, queuing time, route establishment time etc. A network with minimum average end to end delay offers better speed of communication.

$$= \sum t_{PR} - \sum t_{PS}$$

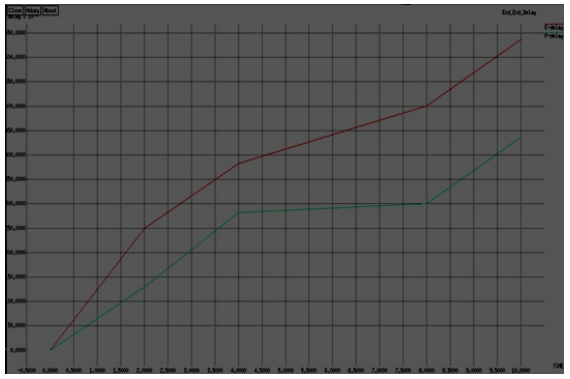
Where, tPR – Packet Receive Time, tPS – Packet Send Time.

Table 4 Delay in the presence of malicious nodes (Attack) and after prevention

Time(ms)	Delay(Attack)	Delay(Prevention)
2	0.250	0.130
4	0.382	0.282
8	0.500	0.300
10	0.636	0.436

From the above table, we can see that the Delay is reduced after applying Master AODV.

X-Graph for Delay



X-axis Time Y-axis Delay

Conclusion

The proposed Master AODV is a modified AODV routing protocol which has improved the performance of the MANET by increasing the Throughput and PDR and reducing the Delay and Packet drop ratio when there is a Grayhole attack.

References

1. Rupinder Kaur and Parminder Singh Review of Black Hole and Gray Hole Attack . The International Journal of Multimedia & Its Applications (IJMA) Vol.6, No.6, December 2014
2. Chatterjee, N., Mandal, J.K.: Detection of blackhole behaviour using triangular encryption in NS2. 1st International Conference on Computational Intelligence: Modeling Techniques and Applications (CIMTA), Procedia Technology, vol. 10, 2013; pp. 524–529.
3. K.Madhuri, Dr.N.Kasi Viswanath Implementation of Postion based technique to prevent Worm hole attack in AODV Routing protocol for MANET International Journal and magazine of Engineering, Technology, Management and Research.Vol 5 2016; pp-11-14.
4. Kamini Singh, Gyan Singh and Arpit Agrawal. Article: A Trust based Approach for Detecting and Preventing Wormhole Attack in MANET. International Journal of Computer Applications 94(20):1-5, May 2014.
5. Tan, S., Kim, K.: Secure route discovery for preventing black hole attacks on AODV-based MANETs. International Conference on ICT Convergence (ICTC), Jeju, Korea2013; pp. 1027–1032.
6. Thachil, F., Shet, K.C.: A trust-based approach for AODV protocol to mitigate blackhole attack in MANET. International Conference on Computing Sciences (ICCS), Phagwara, 2012; pp. 281–285.
7. Kant, R., Gupta, S., Khatter, H.: A literature survey on black hole attacks on AODV protocol in MANET. Int. J. Comput. Appl. 2013; 80(16), 22–26.
8. Ehsan, H., Khan, F.A.: Malicious AODV: implementation and analysis of routing attacks in MANETs. 11th IEEE International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom), Liverpool, UK, 2012; pp. 1181–1187.
9. Amol A.Bhosle,Tushar P.Thosar,Snehal Mehatre Black hole and Worm hole attack in routing protocol AODV in MANET
10. Ankita M.Shendurkar, Prof. Nitin R.Chopde A Review of Black Hole and Worm Hole Attack on AODV Routing Protocol in MANET International Journal of Engineering Trends and Technology (IJETT) – Volume 9 Number 8 - Mar 2014.