ISSN: 2321-7782 (Online)
Impact Factor: 6.047

Volume 4, Issue 8, August 2016

International Journal of Advance Research in Computer Science and Management Studies

Research Article / Survey Paper / Case Study

Available online at: www.ijarcsms.com

# Self Organized Security Aware Routing Over Mobile Adhoc Network

**Sunil Dutt**[1]
M.Tech Scholar
Department of Computer Science & Engineering
Om Institute of Technology and Management
Hisar, Haryana – India

**Dr. Anuj Kumar Sharma**[2]
Associate Professor
Department of Computer Science and Engineering
Om Institute of Technology and Management
Hisar, Haryana – India

***Abstract: Mobile ad hoc networks operate in open environment and there is no centralized controller to monitor the network operations so it is quite easy to intercept the communication over these networks by introducing active and passive attacks. In this paper, the impact of Grayhole attack over AODV routing protocol is analysed and a prevention scheme is introduced to overcome from the compromised situation. We will also analyse the behaviour of routing protocol by varying the attacker's node density variation under the various constraints i.e. Throughput, routing load and PDR.***

***Keywords: AODV, Security Threats, Grayhole, MANET.***

## I. INTRODUCTION

Mobile ad hoc network is formed by group of self-organized and independent nodes those do not depends upon any sort of infrastructure for communication purpose. This type of networks support various advance features i.e. Mobility and Scalability etc. Nodes can freely change their current position thus results in random deformation in network topology. Nodes can join and leave the existing network without any prior information thus results in unstable network condition but scalable network can adopt the dynamic behavior of the nodes. Open network operations invite some sort of security threats which can be active or passive in nature. Any unauthorized node can join the network and can interrupt the entire network operations [1] [2][3][4] .

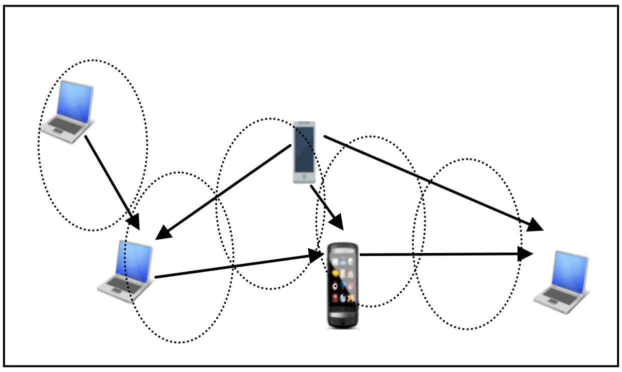
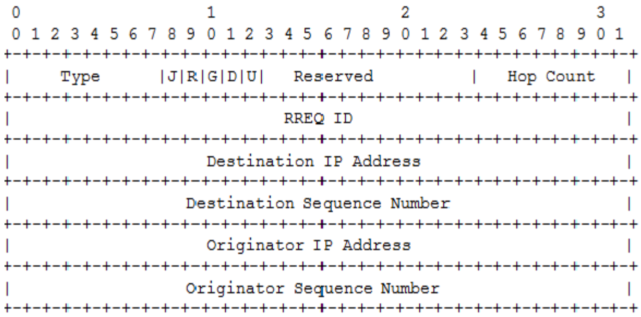


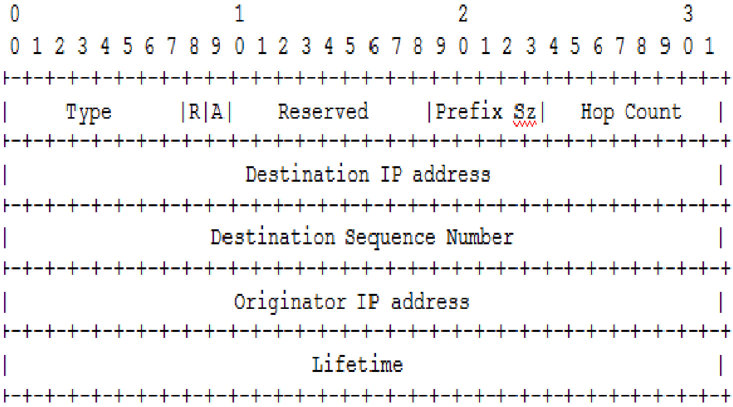
Figure1. MANET

AODV Message Format



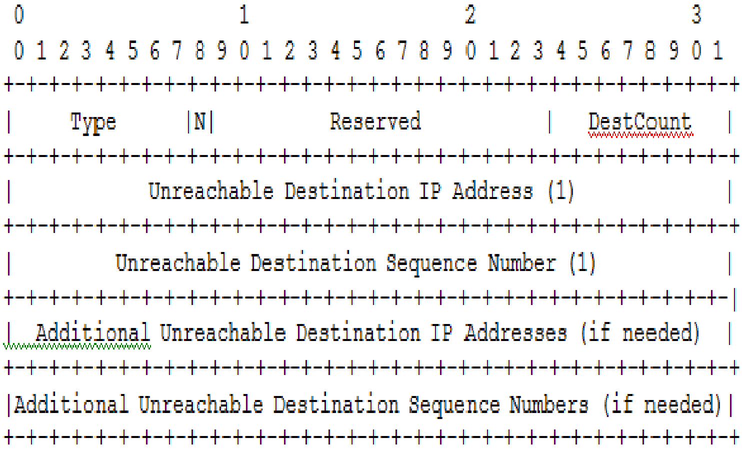
```
  0                   1                   2                   3
  0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
 +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
 |     Type      |J|R|G|D|U|   Reserved          |   Hop Count   |
 +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
 |                            RREQ ID                            |
 +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
 |                    Destination IP Address                     |
 +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
 |                  Destination Sequence Number                  |
 +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
 |                    Originator IP Address                      |
 +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
 |                  Originator Sequence Number                   |
 +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Figure:2 AODV RREQ Message Format[5]



```
  0                   1                   2                   3
  0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
 +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
 |     Type      |R|A|    Reserved     |Prefix Sz|   Hop Count   |
 +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
 |                     Destination IP address                    |
 +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
 |                  Destination Sequence Number                  |
 +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
 |                    Originator IP address                      |
 +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
 |                           Lifetime                            |
 +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Figure:3 AODV RREP Message Format[5]



```
  0                   1                   2                   3
  0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
 +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
 |     Type      |N|          Reserved           |   DestCount   |
 +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
 |            Unreachable Destination IP Address (1)             |
 +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
 |         Unreachable Destination Sequence Number (1)           |
 +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-|
 |  Additional Unreachable Destination IP Addresses (if needed)  |
 +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
 |Additional Unreachable Destination Sequence Numbers (if needed)|
 +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Figure:4 AODV RERR Message Format[5]

Attacks over AODV Routing

Modification of RREQ/RREP/RERR

RREQ is used for route discovery and attacker can alter the routing information stored in RREQ and a fake RREP packet can also be generated by broadcasting the highest sequence number to indicate the fresh route. Intruder can also introduce the fake route error messages and redirect the entire traffic to a wrong route. Following are common security threats for ad hoc networks using above information:

- Black hole Attack
- Gray hole Attack
- Flooding Attack
- Sybil Attack

- Spoofing
- Rushing
- DoS [6]

In this research work, Grayhole attack is investigated which is explained below:

Grayhole attack over AODV routing protocol

Gray hole Attack is a similar to black hole attack except it uses selected shortest paths for route paths can drop the selected forwarding hopes only. It can be easily launched over AODV routing protocol because it highly depends on the hope count and sequence numbers. Whenever sender transmits a route request.

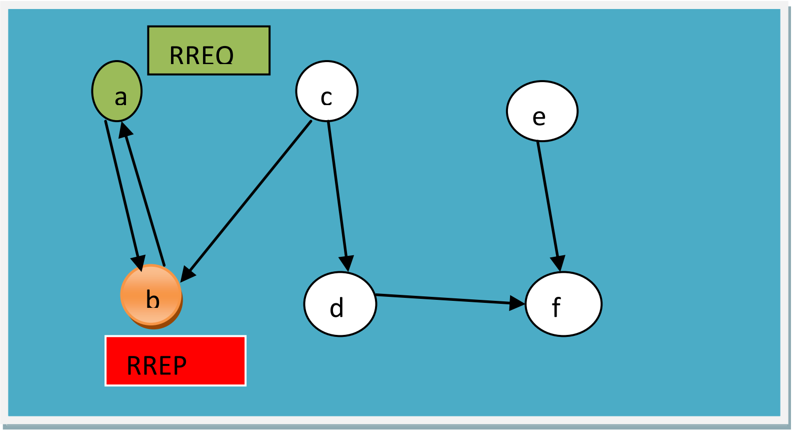


Figure:5 Route interception by intruder node [7]

## II. LITERATURE SURVEY

Ab. A. korba et al. [6] investigated the security issues related to AODV routing over ad hoc networks. Authors explored the various attacks i.e. Black hole, Gray hole, Worm hole, Rushing, DoS, Sybill, flooding and jamming attack. This survey information can be further utilize to develop a robust solution for these attacks.

Kuldeep Singh et al. [8] investigated various security threats (Blackhole, Grayhole, Flooding and Rushing attack) over MANET and their impact on the network performance under the constraints of different parameters i.e. PDR, Delay, routing load, packet loss and Hop count etc. AODV and AOMDV both were used for experimental purpose and simulation results show that each type of attack has different impact over AODV/AOMDV. Rushing attack has a deep impact as compared to other attacks, over AODV whereas AOMDV survives in better way. Current research work can be further used for other protocols i.e. DSDV/DSR.

TAKUJI TSUDA et al. [9] proposed a malicious node detection method which can easily detect the attack using grouping scheme. To identify the malicious nodes in the given network, a query message is broadcasted over the all possible routes and its score is calculated up to its highest value. Neighbor nodes form small groups and send reply and if a reply does not match with the other replies, then it indicates that specific group may have a malicious node and query it is intercepted by intruder nodes and they alter the route request with their own and send its fake reply with minimum delay. After receiving the route reply, legitimate nodes just update their routing tables and introduce the intruders in the network. After all, node starts transmission of data which is selectively dropped by the intruder nodes and only few packets search is limited upto that group only, thus lead to final the identification of the attacker node. Proposed scheme is limited upto the detection of malicious node query it is intercepted by intruder nodes and they alter the route request with their own and send its fake reply with minimum delay. After receiving the route reply, legitimate nodes just update their routing tables and introduce the intruders in the network. After all, node starts transmission of data which is selectively dropped by the intruder nodes and only few packets search is limited upto that group only, thus lead to final the identification of the attacker node. Proposed scheme is limited upto the detection of malicious nodes only.

Zakir Ullah et al. [10] explored the challenges related to existing threats and the Trust management over ad hoc networks. Trust management starts after the Trust establishment which is calculated on the basis of network status and node characteristics etc. Investigation results conclude that Trust establishment between nodes should also consider other parameters i.e. bandwidth consumption, data processing time etc. Security threats can be identify on the basis of different parameters i.e. behavior pattern, data manipulation and identical routing information exchange.

Jianping Yao et al. [11] explored the behavior of compromised network and developed a secure routing scheme for multihop wireless networks. This method calculates the path on the basis of the probability of secure links. Simulation results show that proposed method can establish the secure routing paths between nodes and it can be further extended to support the different routing protocols.

S. Verma et al. [12] explored the gray hole attack over VANETs under the constraints of Throughput, delay, routing load and PDR. Simulation results show that proposed scheme can recover the network resources from attack but it also enhances the PDR, delay and load etc.

S. V. Vasanthaet al. [13] developed a method to identify the malicious routes between sender and intermediate node. After recognizing the false routes, it can also rebuild the shortest paths for communication. It can detect the black hole/gray hole attacks using ACK packets. Simulation results show its performance in terms of improved PDR w.r.t. node density.

A. Lupia [14] et al. enhanced the existing SAODV by introducing the concept of trust management to prevent the network from gray hole attack. Using trust values for routes, false REQ/RREP can be ignored and finally a trusted path can be formed. Simulation results show that proposed scheme consumes less energy as compared to SAODV.

Y. Patil et al. [15] did a survey related to various security threats related to MANET. They explored Black hole, Gray hole and Denial of services attacks and their impact over the transmission. Survey shows that it is very challenging to distinguish bet normal packet drop and routing packet drop. It is also difficult to recognize the Grayhole attack due to selective packet drops. Recognition of legitimate/ intruder nodes is a another issue. Nodes can be identify on the basis of their trust values but in case of compromised network, malicious node can update its trust value automatically. Current security analysis data can be used to develop a security framework.

Ali Alheeti et al. [16] detected the gray hole/ rushing attack over VANETs and proposed a neural network based IDS to prevent the network from such kind of attacks. It monitors the communication between RSUs and multiple vehicles and detects the false alarms related to packet drops and finally this data is used to build traces for analysis purpose. Simulation results show that it can reduce the ratio of false alarms and increase the attack detection ratio.

WANG Yajun et al. [17] developed a scheduling method for packet transmission. This method uses secrecy rate for each node. Transmission schedule can be made upon the basis of the highest values of secrecy rate. It can also adopt the round-robin scheduling scheme and it can arrange all nodes as source and destination pairs. Simulation results show that it can perform even in case of compromised network and it is quite difficult to intercept the value of secrecy.

## III. Simulation Setup

| Simulation Parameters | Parameter Values |
|---|---|
| Multicast Routing Protocol(s) | AODV |
| Terrain | 1200x1200 |
| Node Density | 30 |
| Intruder Node's density | 1,2,4 |
| MAC Protocol | MAC 802.11 |
| Traffic Type | CBR |
| Packet Size | 512 |
| Sampling Interval | 0.1 seconds |
| Simulation Time | 10 seconds |
| Network Simulator | NS-2.34 [18] |
| Simulation Scenario(s) | a. Normal Network Environment<br>b. Compromised Network Environment by Grayhole Attack<br>c. Proposed Scheme for Detection/Prevention of Grayhole Attack |

Table:1 Simulation Scenario

## IV. Purpose Scheme

Grayhole attack is the extension of black hole attack, in which malicious nodes behave like a legitimate node and do not respond during route discovery phase and after that modify the routing data related to destination by altering sequence number. It is difficult to trace this attack at the time of route discovery but later on it can be detected on the basis of the different factors i.e. abnormal packet drop by a specific node, modified sequence number that does not belong to routing table (that is introduced by malicious node) etc . In our proposed, information related to each packet drop and continuity of sequence numbers is analyzed. If generated sequence numbers are in a particular series, then packet drop is ignored. If upcoming sequence number is not in a particular series and its value is very high as compared to the previously generated sequence numbers that indicates it is injected by malicious node and packet drop threshold value for that node is verified and finally, it is declared as malicious node. This node can dynamic change its behavior, so on the basis of number of packet dropped, final value of Threshold and violation of sequence number chain routing information is altered and that node becomes isolated and can't join the network again. Our proposed scheme also works, if number of malicious node's density varies but it is quite difficult to capture single malicious node.

Sequence number chain prediction

N: total number of nodes

T: total duration of communication

SN: Maximum sequence numbers those can be generated

For each node possible destinations Di: N*m

Di destination, total required sequence no.  SCN: D*T

e.g. for 30 nodes, total destinations are 30*30=90 if time duration is 10seconds, then possible sequence numbers , 90*10=900 can be generated, and new sequence is just higher than the previous one, to keep the track of fresh route. So finally we can predict a chain of all possible sequence numbers. If any node generates a sequence number that does not belong to the predicted sequence numbers, it can be easily identified.

```
If (current_SEQ_No<= SCN(s) && current_SEQ_No==Hqscn)

{

        PDS:N;

}

else {

        Hqscn==true;

If (PDS)

{

        Thv++;

}}
```

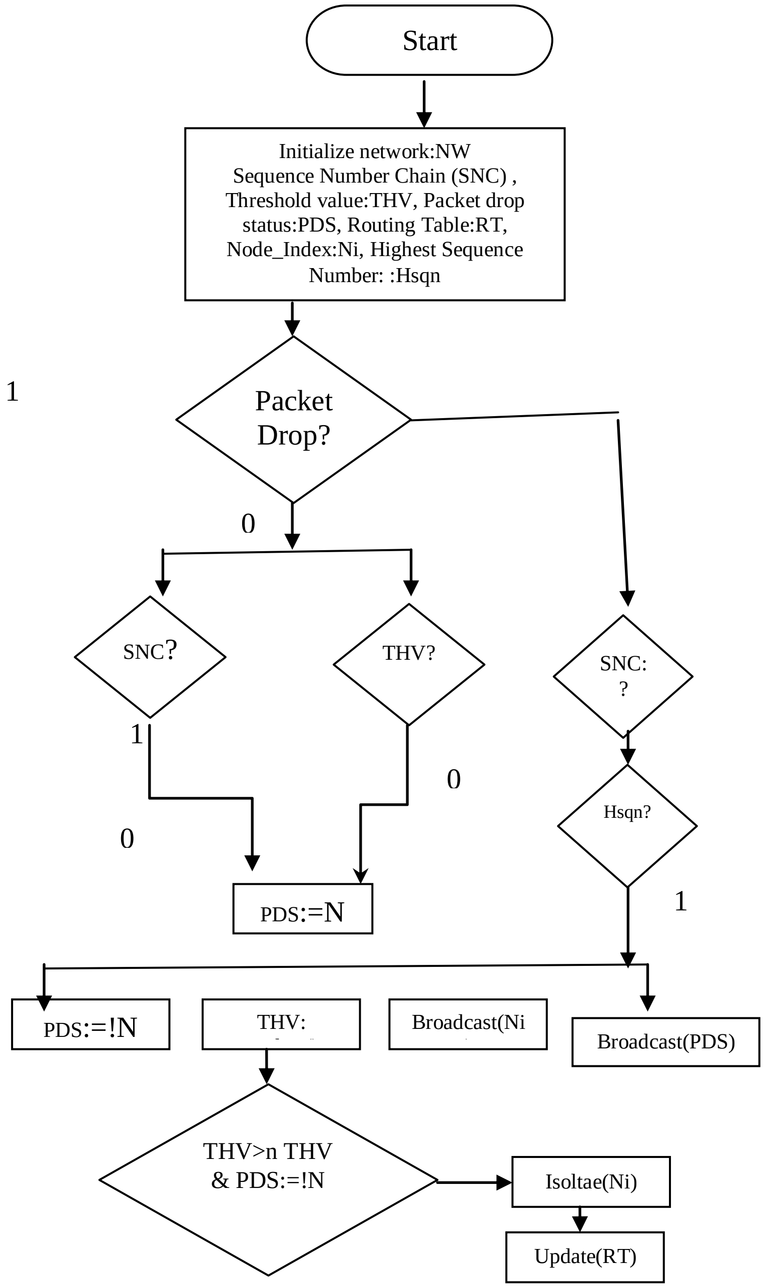


Figure: 6 Proposed Scheme

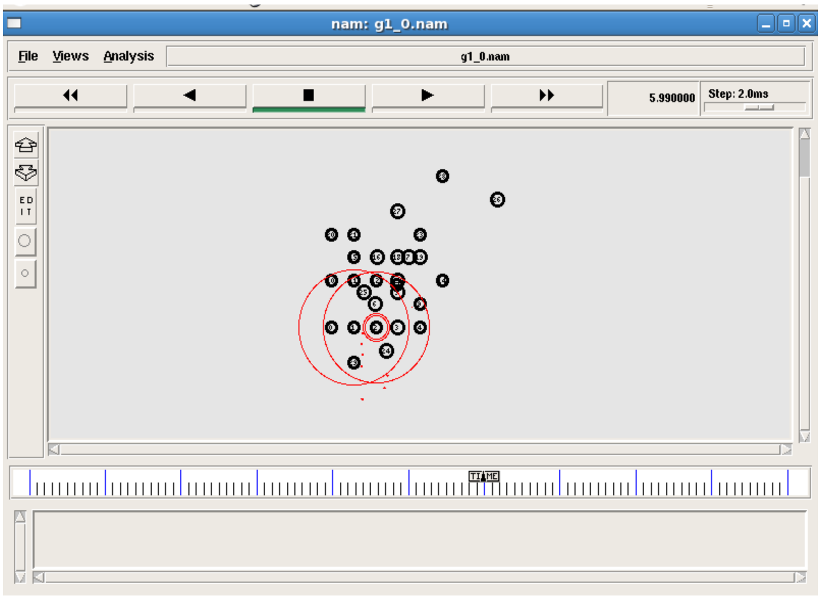


Figure: 7 Packet dropped due to Grayhole attack

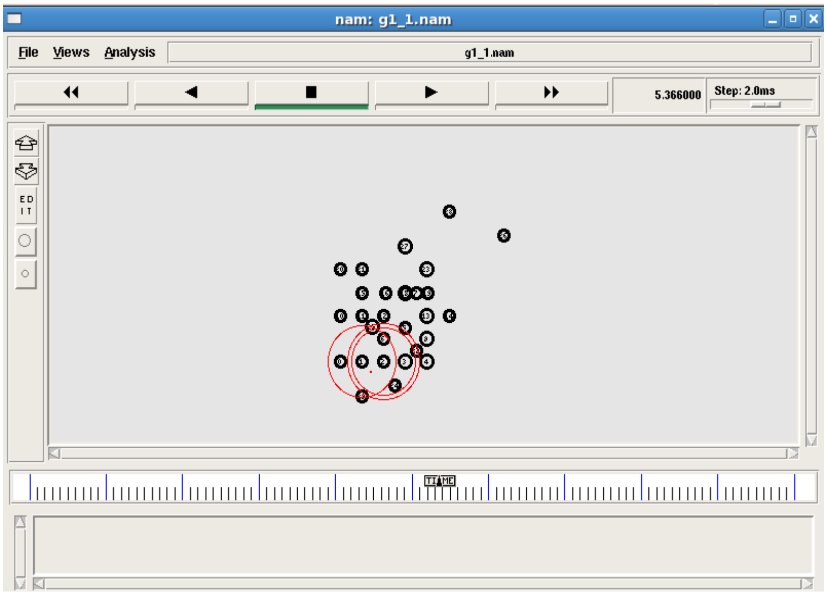


Figure: 8 Proposed Scheme

## V. Simulation Results

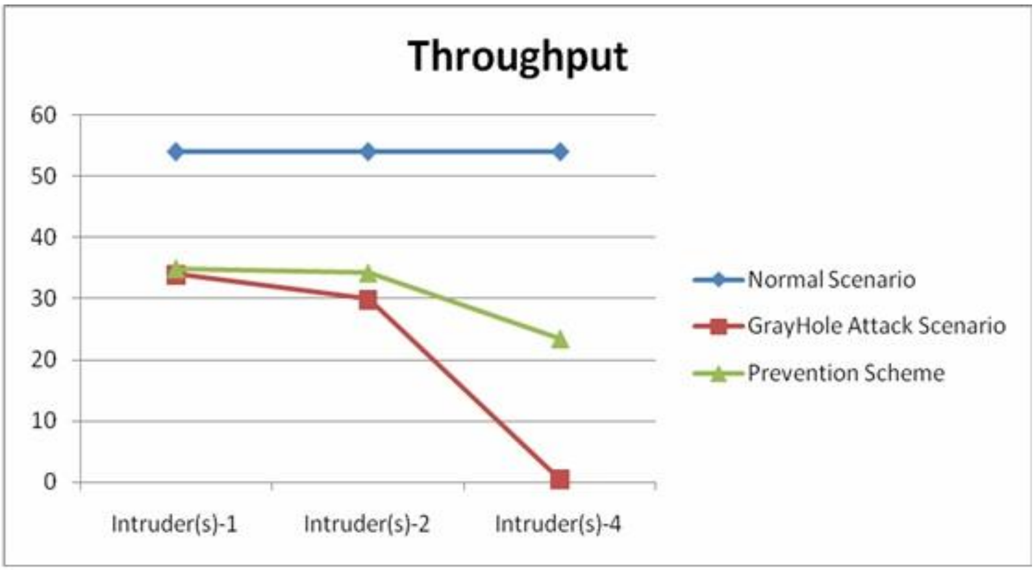


Figure:9 Throughput

Figure: above shows the Throughput of AODV protocol. In normal network environment, Throughput is 54 bps, under compromised network, in the presence of single intruder node, it reduces upto 34bps, in case of 2 intruders, it further reduces upto 29.9 bps and finally it is reduced upto 0.4 bps, in the presence of 4 intruder nodes.

In the presence of single intruder, proposed scheme can recover the Throughput upto 34.9 bps, with two intruder nodes, it can maintain Throughput upto 34.2 bps and in case of four intruders, it can recover Throughput upto 23.5 bps.

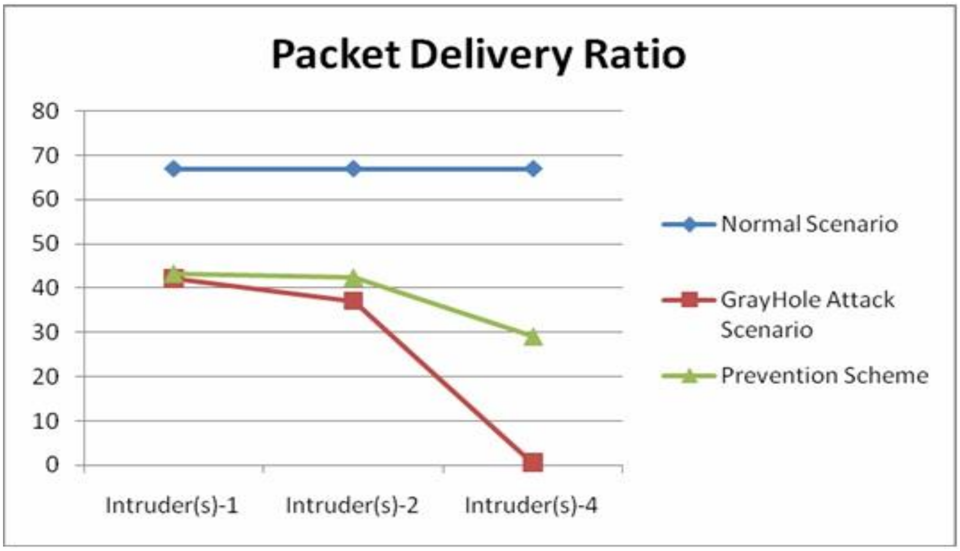


Figure:10 Packet Delivery Ratio

Figure above shows the Packet Delivery ratio, In case of normal network environment, PDR is 66.9975186%, in compromised network, it varies w.r.t. intruder node’s density. In case of single intruder node, it reduces upto 42.1836228%, with two intruders, it is 37.0967742 and four intruders reduce it upto 0.49627792%.

Proposed scheme recovers from attack and in the presence of single intruder, it is 43.3002481%, with two intruders, it is 42.4317618% and with four intruders, it is 29.1563275%.

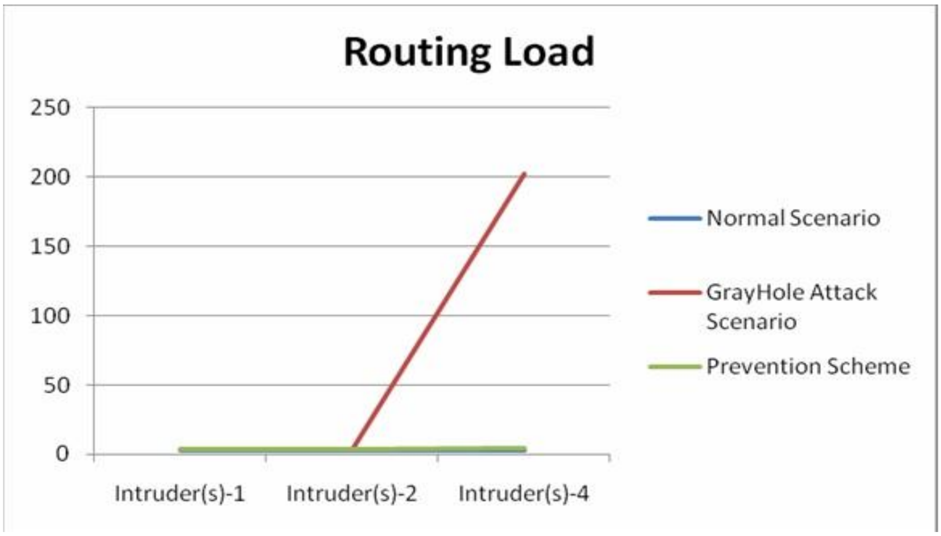


Figure:11 Routing Load

Figure: above shows the routing load variations under different simulation scenarios. It is 2.49259259, in normal network environment but increased upto 202.5, in case of compromised network. Using proposed scheme, it is reduced upto to 4.42978723.

## VI. Conclusion

This research work is related to detection and prevention of Grayhole attack over MANET using AODV routing protocol. As per the literature survey, it can be observed that various researchers have already developed the different solutions to secure the MANET but each have its own strength and limitations. A self-organized Grayhole detection scheme was proposed in this research work. Proposed scheme analysis the routing information as well as the node behavior. Attack detection at node level has a advantage over the existing scheme i.e. traffic analysis can be performed at node level and if there is any change in routing information, entire network is informed. Analysis is performed using sequence number, route discovery, packet forwarding and packet drop. If a packet is forwarded but it is intentionally dropped, then threshold value is updated and each node is aware from this information. If frequent changes occur in sequence number that is also monitored because AODV uses these sequence numbers to keep the information about fresh routes but in case of gray hole attack, selected routes are observed and highest fake sequence number is introduced and replaced with the fresh one and after capturing the route information, finally forward data is dropped at that route.

Now we discuss the simulation results of proposed scheme under the constraints of various parameters i.e. Throughput, Packet delivery Ratio and Routing Load. In normal network environment, Throughput is 54 bps, but during attack phase, if one intruder node is active then, It reduces upto 34bps, in case of 2 active intruders, it further decreased upto 29.9 bps and finally it is reduced upto 0.4 bps due to the four intruder nodes which have the highest impact over the network performance.

Proposed scheme can detect and recover from attack and maintains Throughput upto 34.9 bps, with two intruder nodes, It can maintain Throughput upto 34.2 bps and in case of four intruders, it can recover Throughput upto 23.5 bps.

In case of normal network environment, PDR is 66.9975186%, in compromised network; it varies w.r.t. intruder node’s density. In case of single intruder node, it reduces upto 42.1836228%, with two intruders, it is 37.0967742 and four intruders reduce it upto 0.49627792%.

Proposed scheme recovers from attack and in the presence of single intruder, it is 43.3002481%, with two intruders, it is 42.4317618% and with four intruders, it is 29.1563275%. Routing load variations under different simulation scenarios. It is 2.49259259, in normal network environment but increased upto 202.5, in case of compromised network. Using proposed scheme, it is reduced upto to 4.42978723.

As per the above discussion, it can be observed that it is quite difficult to detect the Grayhole attack but using multiple constraints against attack, it can be detect and prevented. Results show that attack intensity varies w.r.t. density of intruder nodes and it can also be analyzed that our proposed scheme’s results also vary w.r.t. intruder’s density. In the presences of single intruder, it is difficult to detect the attack at early stage because three are little bit changes in Thresh hold value, sequence number and forwarding packet drop ratio, but in case of four intruders, all values frequently altered and updated and it is easy to detect and prevent the attack.

## References

1. M. Rmayti, Y. Begriche, R. Khatoun, L.Khoukhi, D. Gaiti, "Denial of Service (DoS) Attacks Detection in MANETs Using Bayesian Classifiers",SCVT, IEEE-2014, pp. 7-12.
2. Mazda Salmanian, Peter C. Mason ; Joanne Treurniet ; Jiangxin Hu, "A modular security architecture for managing security associations in MANETs", MASS, IEEE, 2010, pp.525 – 530.
3. Ashish Shrestha; Firat Tekiner, "On MANET Routing Protocols for Mobility and Scalability",International Conference on Parallel and Distributed Computing, Applications and Technologies, IEEE-2009, pp.451 – 456.
4. Suresh Kumar , Gaurav Pruthi ; Ashwani Yadav ; Mukesh Singla, "Security Protocols in MANETs", 2012 Second International Conference on Advanced Computing & Communication Technologies, IEEE-2012, pp-530 – 534.
5. Aarti, S. S. Tyagi, "Study of MANET: Characteristics, Challenges, Application and Security Attacks ", IJARCSSE, Vol. (3) 5, 2013.
6. Amara korba Abdelaziz, Nafaa Mehdi, Ghanemi Salim, "Analysis of Security Attacks In AODV", IEEE-2014, pp. 752 – 756.

7. Ramesh babu B, Meenakshi Tripathi , Manoj Singh Gaur, Dinesh Gopalani, Dharm Singh Jat, "Cognitive Radio Ad-Hoc Networks: Attacks and Its Impact", IEEE-2015, pp.125-130.
8. Kuldeep Singh, Amanat Boparai, Vrinda Handa, Sudesh Rani, "Performance Analysis of Security Attacks and Improvements of Routing Protocols in MANET", IEEE-2015, pp-163-169.
9. TAKUJI TSUDA, YUKA KOMAI, TAKAHIRO HARA, AND SHOJIRO NISHIO, "Top-k Query Processing and Malicious Node Identification Based on Node Grouping in MANETs", IEEE-2016, pp-993-1007.
10. Zakir Ullah, Muhammad Hasan Islam,Adnan Ahmed Khan "Issues with Trust Management and Trust Based Secure Routing in MANET", IBCAST, IEEE-2016, pp-402-408.
11. Jianping Yao, Suili Feng, Xiangyun Zhou,Yuan Liu, "Secure Routing in Multihop Wireless Ad-hocNetworks with Decode-and-Forward Relaying", IEEE Transactions on Communications, pp-1-12.
12. S. Verma, Bhawna Mallick , Poonam Verma , "Impact of Gray Hole Attack in V ANET ", NGCT-IEEE, 2015,pp.127-130 .
13. S. V. Vasantha, A. Damodaram, "Bulwark AODV against Black hole and Gray hole attacks in MANET", ICCIC, IEEE-2015, pp.1-5.
14. A. Lupia, Floriano De Rango,"Energy consumption evaluation of SAODV with trust management scheme under gray-hole attacks", WTS, IEEE-2015, pp.1-8.
15. Y. Patil, Ashok M Kanthe, "Survey: Comparison of mechanisms against denial of service attack in Mobile Ad-Hoc Networks", ICCIC, IEEE-2015, pp.1-5.
16. Ali Alheeti, Anna Gruebler, Klaus D. McDonald-Maier, "On the detection of grey hole and rushing attacks in self-driving vehicular networks", CEEC-IEEE-2015, pp-231-236.
17. WANG Yajun, LIAO Tongqing, WANG Chuanan, "An anti-eavesdrop transmission scheduling scheme based on maximizing secrecy outage probability in ad hoc networks", Wang Yajun; Liao Tongqing; Wang Chuanan China Communications, China Communications, IEEE, Vol.13(1), pp- 176 – 184.
18. http://www.isi.edu/nsnam/ns/.

## 19. AUTHOR(S) PROFILE

**Sunil Dutt,** received Bachelor’s Degree in Mathematics from Kurkshetra University Kurkshetra, Haryana, India, in 2006. Having been Master of Computer Application student for 3 years in Maharishi Dyanand University Rohtak, Haryana, India. He determined to pursue M.tech (Computer Science and Engineering) Degree in 2014. He is currently an M.Tech Scholar in Om institute of Technology and Management affiliated from Guru Jamheshwer University of Science & Technology, Hisar, Haryana, India. His research interest include Mobile Adhoc network with an emphasis on prevention and Detection of Security attack on Manet.

**Dr. Anuj Kumar Sharma,** received his Ph.D degree in Computer Science from Lucknow University Lucknow (Uttar pardesh, India) and M.Tech and BE in computer Science and Engineering from Ch. Devi Lal University Sirsa, Haryana, and Maharishi Dayanand University,Rohtak respectively. He joined as lecturer in Computer Deptt. “Shri Baba Mastnath Engg. College Asthal Bohar (Rohtak)” in 2003 after that Worked as lecturer in Computer Deptt. “The Technological Institute of Textile & Sciences Bhiwani in 2003. He joined as Assistant Professor in CSE Deptt in BRCM college of Engg. & Tech. Bahal in 2009, Presently working as Professor (CSE) in Om Institute of Tech. & Mgt. Hisar, Haryana. Dr. Anuj kumar sharma has extensive research experience and published widely in computer networking and Security research. His research interest includes computer networks security, wireless sensor communication and networking.