ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

*(An ISO 3297: 2007 Certified Organization)*

**Vol. 3, Issue 9, September 2015**

# A Modified Approach for Secure Routing Mechanism in MANET

Er. Rashmi Munjal, Er. Ravi Kumar

M. Tech Student, Dept. of CSE, GIMT, Kurukshetra University, Kurukshetra, India

Assistant Professor, Dept. of CSE, GIMT, Kurukshetra University, Kurukshetra, India

**ABSTRACT:** MANETs are known to be less infrastructure and emerging networks, where some work had been done in recent years while they still have many areas of improvement with advancing technology. Technological change makes these networks more as improving capacity to both exploration areas for MANETs are increasing day by day. Security is the main problem in these networks are lacking from the beginning, while many of the safe approaches are proposed and implemented there is still room for improvement in the MANET. In this paper, an approach to security of MANET is implemented and the results obtained after the simulation are discussed in the results section.

**KEYWORDS**: attacker detection; Manets; network recovery; RREP update; Route Update, Security

## I. Introduction

Mobile ad-hoc networks are building blocks for new technologies like self driving cars and intelligent vehicle concept. These networks have improved since the day they are developed and standardized. The standardization process becomes more useful when these techniques are adopted by the scientific community. The new weapons systems, military strategic requirements, vessels and transportation systems, the requirements of security measure in advance and cheaper technologies such as GPS positioning tracker and other advances in technology provides great scope for improving magnets. Improvements are made in a selected field by researcher and extend for the rest of the researchers, the research methodology to maintain the increasingly complex process. From these complex processes, while many improvements gaps or deficiencies become far behind. In the proposed work, this type of deficiency is studied, analysed and work. This provides improvement in the desired areas of routing and network security, thus providing a more reliable network structure.

## II. Related work

Anuj Gupta K., (2011) [19] in its "Review of several routing protocols for MANETs" author claims that routing in MANETs is a difficult task and has received an enormous amount of attention from researchers around the world. To overcome this problem a number of routing protocols have been developed and the number is increasing day by day, the comparison is provided based on the methodologies and routing information used to make routing decisions.

The protocols are divided into three main categories: (i) the source started, (ii) the table driven, (iii) hybrid protocols. For each of these classes has been reviewed and compared several representative protocols, the main differentiating factor between the protocols is the way of the pursuit and maintenance of routes between origin-destination pairs.

Dr. Karim Konate, Abdourahim Gaye (2011) [18] in the "Analysis of Attacks in mobile ad-hoc networks: Modelling and Simulation", the author analyzes various attacks and counter-measure Manet in network routing protocol ad-hoc mobile. Author has done a simulation of certain attacks as Black Hole, saturation bandwidth and mathematical models have been proposed.

Qiu Xiufeng, Liu Jianhua, Liu Jianwei, (2012) [17] in his article "Design and implementation of special network protocol simulation system safe," he says, because the cost of analysis and design of secure network protocols Directors hoc in real network environment is huge, has great importance for the development of a simulation system that can analyze the performance of different security protocols Ad-hoc network. Based on analysis of specific requirements for Ad-hoc secure network protocol simulation, this paper designed and implemented a simulation system that integrates the functions of generation of network topology, the secure protocol settings, creating flows attack data and events,

DOI: 10.15680/IJIRCCE.2015. 0309030

generating simulation scripts automatically run attacks and comparing the performance of protocol, etc. Through comparative analysis of delay, Overhead Control, Performance, Packet Loss Rate, package delivery and jitter simulation results of different protocols running insurance under different attacks, the system can perform the analysis of performance of various secure protocols of Ad-hoc network, and demonstrate the dynamic changes of the network under attack in an animation. A simulation system protocol secure network Ad-hoc was designed and implemented, which integrates the functions of generation network topology, configuring secure protocol, creating data flows and events of attack, producing scripts simulation automatically running attacks and comparing the performance of protocol in MATLAB.

Prinima Ms. Gupta, Dr. RK Tuteja, (2010) [15] in "Design Strategies for Implementation in Linux AODV" building a mobile network nodes, nodes can join and leave at any time, and changes in topology dynamically. Routing in a MANET is difficult due to the dynamic topology and the lack of an existing fixed infrastructure. In this article, we explore the difficulties encountered in the application of MANET routing protocols in real operating systems, and study the common requirements imposed by MANET routing services on the underlying operating system. In addition, implementation techniques explained AODV protocol to determine the necessary events, such as: IGMP, Kernel Modification, and filter network. Field studies using the AODV routing protocol have so far been limited to devices running the Linux operating system, because all have developed the current implementations of AODV for that platform. AODV works great for both high mobility and high traffic load network, making it one of the most interesting candidates among ad-hoc routing protocols today. The implementation of a routing protocol is very important to validate its design. Coming up with a clean implementation not only helps to better understand the nuances of protocol, but also allows extensions to explore the design space protocol. In this paper the design possibilities for AODV implementations were analyzed. In addition, this paper analyzes the advantages and disadvantages of each implementation of this architecture in Linux is presented.

Ian D. Chakeres, Elizabeth M.Belding-Roye (2004) [17] in "Routing Protocol AODV Design Implementation" analyzed the design possibilities for AODV implementation. Possible opportunities to benefit from the events include: snooping, modification of the kernel, network filter. In the different sections, each of these possibilities are described and their respective strengths and weaknesses are discussed.

Monika Roopak, Prof. BVR Reddy (2013) [5] in the newspaper "The implementation Black hole attack in AODV routing protocol" author claims that Mobile Ad-hoc networks are a collection of mobile hosts to communicate with each other without any infrastructure. Due to security vulnerabilities of routing protocols, mobile ad hoc networks can be unprotected against attacks from malicious nodes. One of the attacks is the Black Hole Attack on the integrity of the network in this all data packets are absorbed by the malicious nodes. Since the data packets do not reach the destination node because of this attack results in loss of data. In this work we see how to implement black hole attack in Ad-hoc mode protocol on demand distance vector using the network simulator 2.34.

## III. PROPOSED ALGORITHM

### A. *Design Considerations:*

- Network is configured to adopt the new approach
- Nodes are able to calculate the RREP packet arrival time to differentiate between the actual destination and attacker.
- Keeping track of previously used paths in case of RREP.
- Node are able to check the sequence no. of the node.

### B. *Description of the Proposed Algorithm:*

Aim of the proposed algorithm is to avoid the attacker node from degrading the network performance.
Step-1: RREP is used as the medium to assure the Destination.
Step-2: When the network communication stats the network searches for the destination.
Step-3: As RREQ packet is received by the attacker node it instantly generates the reply without checking anything.

DOI: 10.15680/IJIRCCE.2015. 0309030

Step-4: The RREQ packet is forwarded by the other nodes and in the network when it reaches to actual destination the RREP packet is generated.
Step-5: The RREP packet is received by node in the network designated as the source node.
Step-6: Check is made to find out the sequence no. of the RREP packet.
Step-7: The generates time and the sequence no. is checked every time the RREP is received.
If the sequence no. is same as that of entry present in routing table it is discarded
Else if the sequence no. is lesser than that of entry present in the routing table, it means the RREP entry previously made is done with attacker node.
Replace it with the new RREP entry.
Start communication with the new entry in the Routing table.

## IV. PSEUDO CODE

Step 1: Display the network nodes.
Step 2: Configure the network node to work with the help of proposed security mechanism.
Step 3: Network is configured to have the same malicious node as that of normal network under attack.
Step 4: Network is supported with the fix no of source node and destination nodes to setup the communication in the network.
Step 5: Network is adopted to implement the attack while the nodes to recover the network from performance degradation caused by attack.
Step 6: New paths are choose and implemented to avoid the attack nodes.

## V. SIMULATION RESULTS

Th A simulation study was carried out to evaluate the performance of AODV, AODV under attack and our purposed improved AODV protocol based on the metrics packet drop , packet delay and energy efficiency with the following parameters

**Table 1: Parameters of IAODV, BAODV, AODV**

| **Parameter** | **Value** |
|---|---|
| Radio model | Two Ray Ground |
| Protocols | AODV, IAODV, BAODV |
| Traffic Source | Constant Bit Ratio |
| Packet Size | 512 bytes |
| Area | 750X750 |
| Application | UDP |
| MAC | Mac/802_11 |

In the work, It can count the number of packets dropped at each node including the black hole node. In all scenarios we tested, the same nodes are acting as a source of sending it. For each simulation , Network has taken 20 nodes with fixed topology chosen at random in a flat space of 750 x 750 meters. 9 short simulations were performed in a long-term simulation. In the first simulation, the performance of the network is tested without Black hole attack. Xgraph to evaluate the performance of MANETs (ns-2 built-in tool) was used.

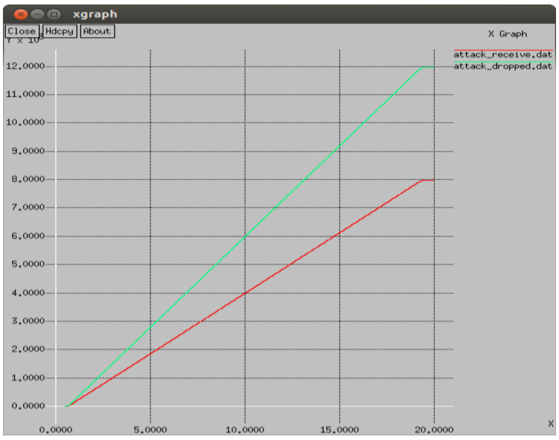
- Receive and dropped Packets

This figure is drawn from receiving packets and dropped packets calculations. The graph is drawn to find the degree of the received packet is the number of dropped packets. The graph to the attack and recovery (proposed algorithm) are represented separately. If decanting attack dropped packets linear scheme is higher.

This sedimentation indicates the number of packets dropped in case of attack is higher and the extension of the received packet is lower. While by examining the proposed algorithm plots the information that is not obtained. of received

DOI: 10.15680/IJIRCCE.2015. 0309030

packets increases and decreases as a result lost packets are the slope of the line decreases and fallen packages decantation line received packet increases.



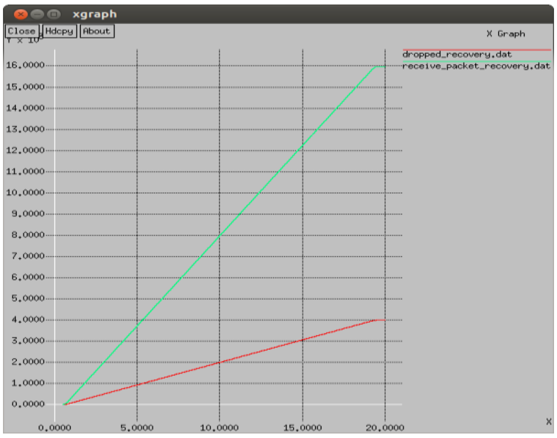
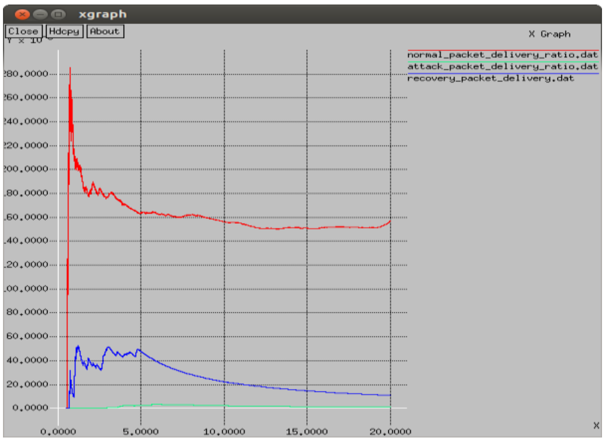


Figure 1: Plot corresponding to attack implementation Figure 2: Plot corresponding to recovery mechanism

- Packet Delivery Ratio:

Packet delivery ratio is a correct measure of the extent that how effective is the attack to affect the network functioning Packet delivery graphs can be plotted as:



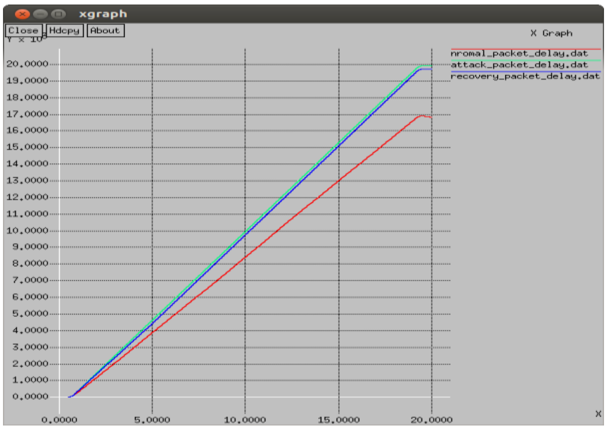


Figure 3: PDR comparision of different approaches Figure 4 : Packet delay plot for three implementations

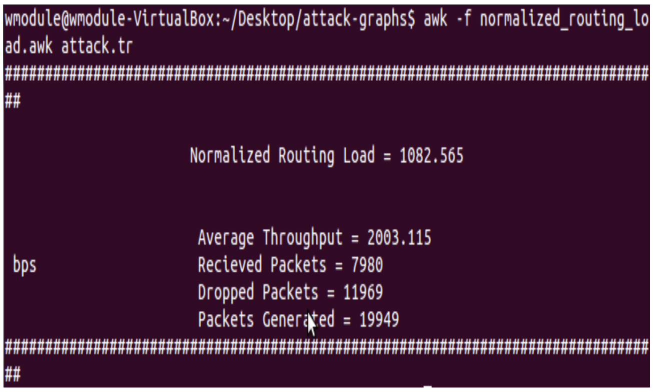
Figure 4 shows the different implementations plot of normal implementation, attack implementation and recovery implementation. The red line shows the normal, green plot shows the attack and blue plot shows the recovery plot.

- Packet Delay:

Packet delay is the measure of the time taken for a packet to reach its destination. Packet delay provides information about the time a packet has to wait for the destination. Figure 5 provides the frame packet delay for the three implementation. The normal fabric, handles simple protocol implementation. The attack plot deals with implementation protocols attack and recovery frame refers to the implementation of the proposed protocol.

- Average values of different parameters:

Average value of different parameter provides summary information on the performance parameters of the various protocols implementations. The mean value of various parameters. Figure 6 provides the frame average value for the three implementation. The various parameters include average average yield receive packets, average packet delivery ratio.

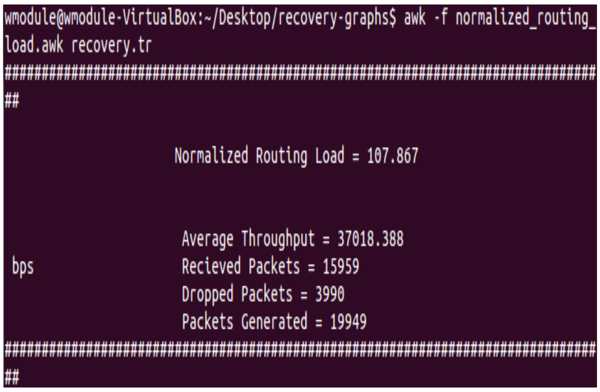


```
wmodule@wmodule-VirtualBox:~/Desktop/attack-graphs$ awk -f normalized_routing_lo
ad.awk attack.tr
################################################################################
##

                        Normalized Routing Load = 1082.565


                         Average Throughput = 2003.115
 bps                     Recieved Packets = 7980
                         Dropped Packets = 11969
                         Packets Generated = 19949
################################################################################
##
```

Figure 5: Average Value for attack implementation



```
wmodule@wmodule-VirtualBox:~/Desktop/recovery-graphs$ awk -f normalized_routing_
load.awk recovery.tr
################################################################################
##

                        Normalized Routing Load = 107.867


                         Average Throughput = 37018.388
 bps                     Recieved Packets = 15959
                         Dropped Packets = 3990
                         Packets Generated = 19949
################################################################################
##
```

Figure 6 : Average Value for recovery (Proposed )

## VI. CONCLUSION AND FUTURE WORK

Implementation of security mechanism in AODV to prevent the attack on the network by initiating a new path route discovery. The new route provides more relationship established delivery in less time delievery. It provides higher performance that provides an indication that more packets are delivered to their destination, compared with net that is attack. As a result of energy consumption in the network it is reduced.

## REFERENCES

1. Soufiene Djahel, Farid Naıt-abdesselam, and Zonghua Zhang 2011 “Mitigating Packet Dropping Problem in Mobile AdHoc Networks: Proposals and Challenges” publish in IEEE COMMUNICATIONS SURVEYS & TUTORIALS, VOL. 13, NO. 4, FOURTH QUARTER 2011
2. Seapahn Megerian, Miodrag Potkonjak “Wireless Sensor Networks”
3. Arampatzis, Th, J. Lygeros, and S. Manesis. "A survey of applications of wireless sensors and wireless sensor networks 2005" Publish in IEEE International Symposium on, Mediterrean Conference on Control and Automation. IEEE, 2005.
4. Akyildiz, Ian F., Xudong Wang, and Weilin Wang. "Wireless mesh networks: a survey." Publish in Computer networks 47.4 (2005): 445-487 in ELSEVIER.
5. X. Wu and D. K. Y. Yau, “Mitigating denial-of-service attacks in MANET by incentive-based packet filtering: A game-theoretic approach”, *In Proc. 3rd International Conference on Security and Privacy in Communications Networks*, Nice, France, September 2007.
6. Panos C. Lekkas Randall K. Nichols. “Wireless Security - Models, Threats and Solutions” Mc Graw Hill, 2002
7. Guarnera, M., et al. "MANET: possible applications with PDA in wireless imaging environment." Personal, Indoor and Mobile Radio Communications, 2002. The 13th IEEE International Symposium on. Vol. 5. IEEE, 2002.
8. http://www.dauniv.ac.in/downloads/Mobilecomputing/MobileCompChap11L02MANETPropertiesandSpectrumRequir.pdf
9. Chin, Kwan-Wu, et al. "Implementation experience with MANET routing protocols." Publish in ACM SIGCOMM Computer Communication Review 32.5 (2002): 49-59
10. Bansal, Meenakshi, Rachna Rajput, and Gaurav Gupta. "Mobile ad hoc networking (MANET): Routing protocol performance issues and evaluation considerations." (1999).
11. Routing protocols in ad hoc networks: a survey Azzedine Boukerche, Begumhan Turgut, Nevin Aydin, Mohammad Z. Ahmad, Ladislau B¨ol¨oni, and Damla Turgut1
12. Gorantala, Krishna. "Routing protocols in mobile ad-hoc Networks." *A Master’thesis in computer science, pp-1-36* (2006)
13. *web2.uwindsor.ca/courses/cs/aggarwal/.../Docs/ReportOnGlomosim.doc*
14. http://www.ijmer.com/papers/Vol3_Issue2/BO32845848.pdf
15. Perkins, Charles E., and Pravin Bhagwat. "Highly dynamic destination-sequenced distance-vector routing (DSDV) for mobile computers." *ACM SIGCOMM Computer Communication Review* 24.4 (1994): 234-244
16. Lee, Unghee, Scott F. Midkiff, and Jahng S. Park. "A proactive routing protocol for multi-channel wireless ad-hoc networks (DSDV-MC)." *Information Technology: Coding and Computing, 2005. ITCC 2005. International Conference on*. Vol. 2. IEEE, 2005
17. Ullah, Irshad, and Shoaib Ur Rehman. "Analysis of Black Hole attack on MANETs Using different MANET routing protocols." *A Mater Thesis, Electrical Engineering, Thesis No. MEE* 10 (2010): 62.]
18. De Rango, Floriano, Marco Fotino, and Salvatore Marano. "EE-OLSR: energy efficient OLSR routing protocol for mobile ad-hoc networks." *Military Communications Conference, 2008. MILCOM 2008. IEEE*. IEEE, 2008]
19. http://www.cs.jhu.edu/~cs647/aodv.pdf
20. Johnson, David B., and David A. Maltz. "Dynamic source routing in ad hoc wireless networks." *Kluwer International Series in Engineering and Computer Science* (1996): 153-179.]

## BIOGRAPHY

**Rashmi Munjal** is a Student of M.Tech(CSE) in Geeta Institute of Management and Technology, Kanipla.Her research Interests are MANETS(Mobile Adhoc Networks), Modified Approach in security, NS2 Simulator.