Analysis of Performance Parameters of AODV in Presence of Malicious Nodes in MANET by Varying Nodes Density

Neha Sharma, Shahjahan Ali

Abstract- Nodes are important aspect of Mobile network. Mobile ad-hoc network means any network that is made at the time of need. Ad-hoc network has its own place in networking. Mobility in network makes it more demandable. Nodes are the device that takes part in network or makes network. Nodes behavior describes network configuration. Genuine node insures you proper working of network with best results as throughput or packet ratio. Presence of malicious nodes differs in comparison to genuine node. Malicious node degrades output of network. Performance metrics noted degradation in their quality when malicious node encounters in network. Malicious nodes in different sets of node density affect the network in different way.
Index Terms– MANET; Malicious; Genuine; Density

I. INTRODUCTION

Mobile Ad-hoc Networks is not new but in past years, Mobile Ad-hoc Network got immense attraction. In this modern era every-one wants high speed uninterrupted, secure facilities. MANET has all points to provide previous services only if it consist any secure mechanism. Therefore analysis of MANET network is important to understand what security hazards troubles network. One of the hazards is malicious node. Malicious node works as hazard in network and harm the accuracy of network.

Malicious node degrades the performance of network by dropping data packets. Here in above section the comparison in performance metrics is illustrated to understand effects of malicious nodes in MANET. One more parameter what is taken under this research is variation of number of nodes. So we can also visualize effects of numbers of nodes in performance metrics.

PDR, THROUGHPUT and DELAY are the three parameters which are taken to analyze effects of malicious nodes in Ad-hoc networks.

II. LITERATURE REVIEW

In paper [5] author Ms. Lilu Odera et. al proposed watchdog method to detect misbehaving nodes and used different sets of threshold values. Here in this paper comparison of different node sets is shown w.r.t selfish nodes.

In paper [6] author Sujitha R. proposed intrusion detection mechanism to detect malicious node and thereafter to increase network performance.

In paper [7] author Anil Kumar Gupta and Deepti Mehrortra proposed algorithm to detect malicious nodes so they can never again take part in same network.

Revised Manuscript Received on July 05, 2019.
Neha Sharma, Computer Science Engineering, SRMSCET, Bareilly, India.
Shahjahan Ali, Computer Science Engineering, SRMSCET, Bareilly, India.

In paper [8] author Khurram Gulzar Rana and et. al proposed acknowledgement based approach to authenticate node and to detect misbehaving node. AODV-MDR is proposed in this paper to perform secure transfer of data packets.

III. ROUTING PROTOCOLS

Routing protocols are the key in MANET that is used to provide path to node from source to their destination. In MANET there are three basic routing protocols that are shown in below figure.

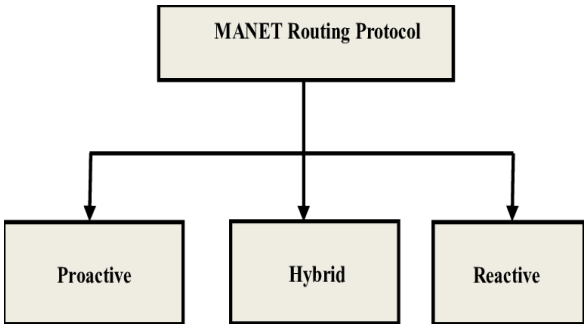


Figure 1: MANET Routing Protocols Classification

A.Proactive Routing Protocol (Table Driven)

Proactive protocols are those protocols that used table of each node to save information about that node. Table is maintained all the time by protocols. This is the reason that overhead of these protocols is high.

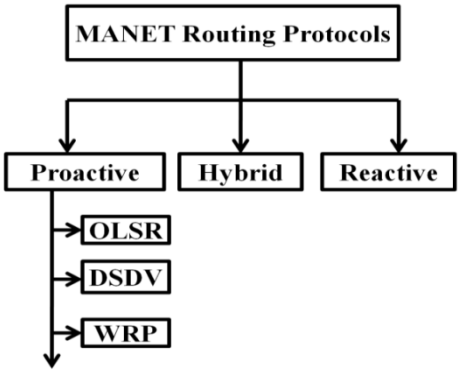


Figure 2: Proactive Routing Protocols Classification [3]

B. Hybrid Routing Protocols

Hybrid routing protocols are combination of both reactive and proactive routing protocols. ZRP, SRP and CEDAR are the example of hybrid protocols.

They provide higher scalability in comparison to other protocols.

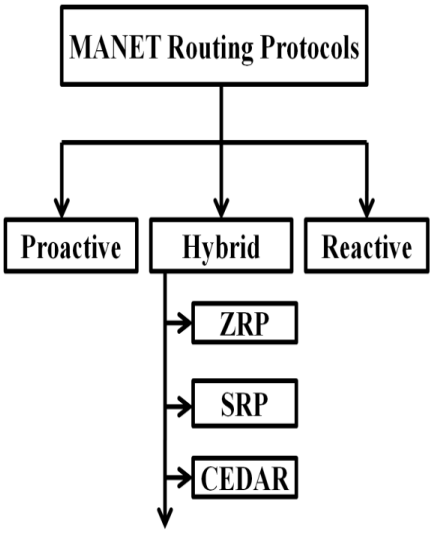


Figure 3: Hybrid Routing Protocols Classification [3]

C. Reactive Routing Protocols (On-Demand)

Reactive routing protocol is better version of proactive protocol. Here in this protocol tables are not maintained in all of the time. But it is updated when it is required. Therefore overhead of protocol is less then proactive routing protocol.

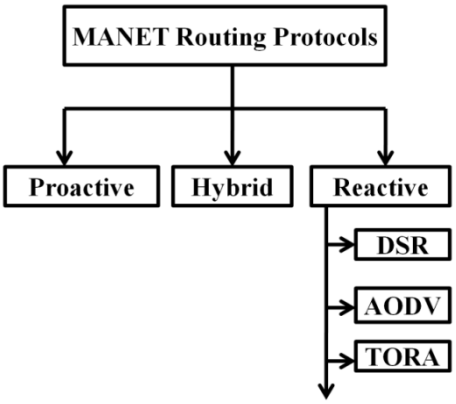


Figure 4: Reactive Routing Protocols Classification [3]

a) AODV

AODV routing protocol is used here in this technique. Sequence number is used in aodv. With the help of sequenced number we can count on genuine node. Malicious node enters in aodv protocol and affects its performance.

IV. PROPOSED WORK

AODV protocol is used to simulate the proposed scenario. AODV protocol is simulated with different node density like 15, 25, 35 upto 55 nodes. Then malicious node is entered in the network and we simulate the AODV protocol with malicious node with different node density. Performance parameter in both scenarios is observed with the help of awk and xgr files. At last with the help of xgraph anf xgr files we plot the outpot for better understanding. The xgraph is added in v section of this paper.

V. RESULT AND ANALYSIS

We simulate the proposed network with the help of network simulator. Here for this NS2.35 is used that is installed in ubuntu 16.04 LTS.

Table 1 Simulation parameters

Area	1000*1000
Routing protocol	AODV
Number of nodes	15,25,…….55
Node mobility	20
Traffic	CBR
Simulation time	20 second

In above table simulation parameters are defined that is used for simulation.

a. PDR

Packet delivery ratio of malicious and non-malicious network can be visualized with the help of below xgraph. Packet delivery ratio is the ratio of packets that are transmit by source node to packets that are received by destined node.

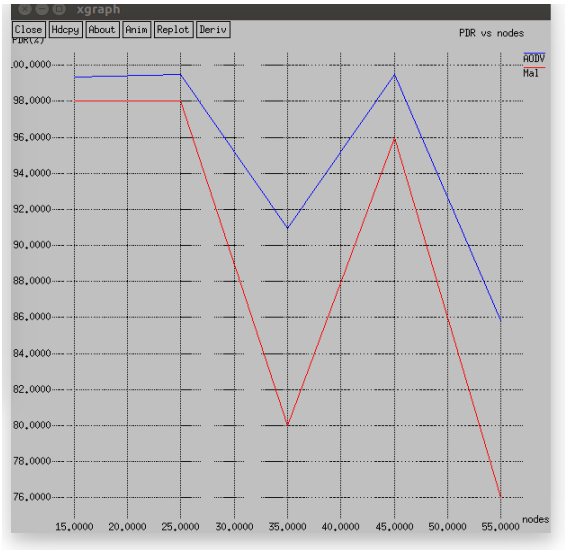


Figure 5: Xgraph of PDR

From the above graph we can analyze that when malicious nodes enters in network PDR is decreased in comparison to AODV. Bule line shows pdr of AODV and red line shows pdr of blue line. As blue line is having high peak then red. It shows malicious nodes degrades packet delivery ratio.

b. Throughput

Throughput of any network is ratio of received data packets to send data packets. Throughput of both malicious and aodv network is shown in below figure.

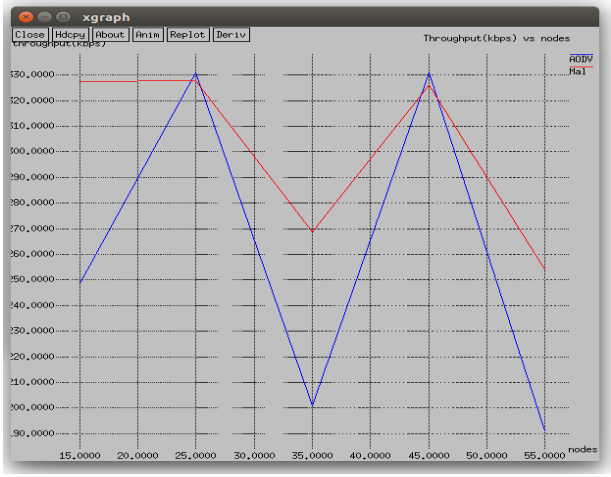


Figure 6: Xgarph of Throughput

Here in above figure throughput of both aodv and aodv with malicious node is plot. In average it shows that due to malicious node throughput of aodv is decreased. Reason of degradation of throughput is malicious node behavior. Malicious nodes receive packets and drop it. So in result throughput is also decreased.

VI. FUTURE WORK

Malicious node can be entering in network in many ways. Like malicious node can be included in network by wormhole attack or gray- hole attacks. All these type of attack inject the network with malicious nodes. So for future work or analysis one can perform analysis of routing protocols in presence of such attacks. Other parameters than pdr, throughput, delay can be taken.

VII. CONCLUSION

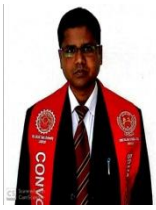
Analysis of malicious nodes shows that with malicious node and without malicious node the output of parameters are differ. From the graph it is shown that malicious nodes have less accuracy then malicious-less networks. Therefore security of MANET becomes fragile in presence of malicious nodes. From the outputs graphs one can understand affects of malicious nodes in network. For security many techniques can be used in MANET. Like secure AODV protocol can be used instead of AODV. For detection of malicious node techniques like watchdog technique can be used. Intrusion prevention system can be used for better results.

REFERENCES

1. Shima Mohseni, Rosilah Hassan, Ahmed Patel, and RozilawatiRazali, “Comparative Review Study of Reactive and Proactive Routing Protocols in MANETs,” IEEE, 2010.
2. Anuj K. Gupta, Harsh Sadawarti, and Anil K. Verma, “Review of Various Routing Protocols for MANETs,” International Journal of Information and Electronics Engineering, vol. 1, no. 3, 2011.
3. Nilesh P. Bobade, Nitiket N. Mhala, “Performance Evaluation of AODV and DSR ON-DEMAND Routing Protocols with Varying MANET Size”, International Journal of Wireless & Mobile Networks, Vol. 4, No. 1, 2012
4. Himadri Nath Saha, Aparjita Chattopadhyay, Debabrata Sarkar, “Review in Intelligent Routing in MANET,” IEEE, 2015.
5. Ms. Liliu Odera and et. al, “Detection and Prevention of Selfish Attacks in MANET Using Dynamic Learning”, IOSR journal of Computer Engineering (IOSR-JCE), 2016.
6. Sujitha R. and et. al, “Malicious Node Detection in MANET”, IJIRSET, February 2014.
7. Anil Kumar Gupta and Deepti Mehrortra, “Detecting and Dealing With Malicious Node Problem in MANET”, IJSER, 2013.
8. Khurram Gulzar Rana and et. al, “Detection of Malicious Nodes in Wireless Adhoc Network by using Acknowledgement based Approach”, ICCNS, 2017.

AUTHORS PROFILE

Ms. Neha Sharma is a research scholar. She is pursuing M.Tech from SRMS CET ,Bareilly from Computer Science Enngineering. She did her B.Tech from Dr. APJAKTU, Lucknow.She published 3 paper yet. One of them is published in SCOPUS INDEXED conference held in Delhi.



Mr. Shahjahan Ali is Assistant Professor in Computer Science department in SRMSCET College. He has 14 years experience in Teaching. He is pursuing Ph.D. from AKTU. He did his Master from GBTU, Lucknow and Bachelor from UPTU, Lucknow. He has published many papers in different international and national journal.