Impact of Network Density on ZRP and Malicious Nodes Detection under Varying Transmission Range and Mobility of Nodes in Manets

Richa Arora [1], Dr. Swati Sharma[2]

[1]Department of ECE, Universal Group of Colleges, Lalru Mandi PTU Jalandhar, Punjab

[2]Asst. Professor, Department of ECE, Universal group of colleges, Lalru Mandi PTU Jalandhar, Punjab

E-mail- richaarora068@gmail.com

Abstract— A Mobile ad hoc network (MANET) is a continuously self configuring infrastructure-less network of mobile devices connected without wires.

MANETS are extensively used these days for communication and there are various communication networks with different standards and computing techniques, different Zone Routing Protocol by varying transmission range and mobility of MANETS are used. As days are passing by the size of MANETS is increasing day by day and its expansion is inevitable due to its high penetration and popularity for the usage of mobile application but at the same time it is also prone to many attacks and network failure due to technical vulnerability of the network. This paper discuss the impact of network density on ZRP and malicious nodes detection under varying transmission range and mobility of nodes in MANETS. Therefore we need a mechanism which would need to overcome such scenarios. Simulation results shows better results for packet loss ratio, throughput, packet delivery ratio and other parameters by detecting malicious nodes in Zone routing protocol under varying transmission and mobility for proper and smooth functioning of MANETS. Abstract must be of Time New Roman Front of size 10 and must be justified alignment.

Keywords—— MANET, DOS, Mobile Ad-hoc Network ,AODV Protocol, PDR, PLR, RO, Throughput

I.INTRODUCTION

1.1 Mobile ad-hoc Networks:-An ad hoc network is the cooperative engagement of a collection of mobile nodes without the required intervention of any centralized access point or existing infrastructure. Ad hoc networking for commercial uses; however, the main applications lie in military, tactical and other security-sensitive operations. In these applications, secure routing is an important issue. Most of the protocols proposed for Secure Routing are either proactive or reactive. In MANETS mobility is the major issue. There are several problems in routing with mobile ad hoc network like asymmetric links, routing overhead, dynamic topology and inference.

1.2 Zone Routing Protocol:- ZRP is an example of a hybrid reactive/proactive routing protocol based on parameter called routing Zone .ZRP is proposed to reduce the control overhead of proactive routing protocols and decrease the latency caused by routing discover in reactive routing protocols. In ZRP a node proactively maintains routes to destinations within a local neighbourhood which is referred to as routing zone.

2. SECURITY GOALS:- Mobile ad-hoc networks (MANETS) are prone to a number of security threats.

There are five major security goals that need to be addressed in order to maintain a reliable and secure ad-hoc network environment. The mechanisms which are used to detect, prevent and respond to security attacks They are mainly:

(i) Confidentiality: Protection of any information from being exposed to unintended entities. In ad hoc networks this is more difficult to achieve because intermediates nodes receive the packets for other recipients, so they can easily eavesdrop the information being routed.

(ii) Availability: Services should be available whenever required. There should be an assurance of survivability despite a Denial of Service (DOS) attack. On physical and media access control layer attacker can use jamming techniques to interfere with communication on physical channel. On network layer the attacker can disrupt the routing protocol. On higher layers; the attacker could bring down high level services.

(iii) Authentication: Assurance that an entity of concern or the origin of a communication is what it claims to be or from. Without which an attacker would impersonate a node, thus gaining unauthorized access to resource and sensitive information and interfering with operation of other nodes.

(iv) Integrity: Message being transmitted is never altered.

(v) Non-repudiation: Ensures that sending and receiving parties can never deny ever sending or receiving the message.

3. PROPOSED METHOD AND OBJECTIVE

Our proposed method primarily based on detection and isolating of malicious nodes from the zone in a network, so that rest of the genuine nodes can work peacefully. Our approach based on ZRP integrates two main features of varying transmission range and mobility of nodes and detecting malicious nodes in MANETS by utilizing different kinds of centrality of nodes even in highly mobile and disconnection prone scenarios..

4. QoS BASED PERFORMANCE METRICS:-

Quality of Service based performance metrics are designed for detection of malicious nodes under simulation environment. These parameters are as follow:-

4.1 *Throughput*

.

4.2 *PDR*

PDR = TOTAL NO. OF PACKET RECEIVED /TOTAL NO. OF PACKET SEND

4.3 *ENERGY CONSUMPTION*

4.4 *NUMBER OF COLLISIONS*

In a network, when two or more nodes wants to transmit data at the same time network collision occurs. When a packet collision occurs the packet is either discarded or sent back to their originating stations and again retransmitted in a times based sequence to avoid collisions. Collisions can result in loss of packet integrity or can impede the performance of a network. This metric is used to measure such collision in the network.

4.5 *PLR*

Packet loss ratio = Number of lost packet / (Number of lost packet + Number of packets received successfully)

4.6. Node placement strategy:-Node placement strategy is random over 100 nodes.

4.7 Data Rate:- Data rate is set to 2mbps

4.8 Routing layer protocol:-Routing layer protocol is zrp

5. RESULTS AND DISCUSSION

Simulation results shown in table1, parameters of network density with varying mobility rate and transmission range and calculated the throughput and packet delivery ratio which is better. And PDR is calculated after bifurcating the genuine nodes in a network to ensure the quality of services.

Table 1

Parameter	**value**
Routing Load	10.89
Average Delay	0.168
Actual Start Time	87.16 Sec
Supposed Time	0.0 Sec
Simulation Time	200 Sec
Throughput	715.5
Packet Send	30446
Packet Received	29952
Packet Delivery Ratio	98.33%

As the network is running smoothly, the packets are delivered to its maximum value between 90-100% ,but with the introduction of attack its value dropped from 90-100% to 10%.

Similar results are obtained for packet loss, packet received, throughput etc.

When the network is running smooth and fine without any introduction of any attack there is normal communication of packet being send and receive which leads to packet delivery ratio above 90% which can be seen in the session of IDS but when there is an attack occurring there is a sudden dip in throughput as well as PDR about 10% less than normal.

x- axis=Mobility rate

y-axis=PDR

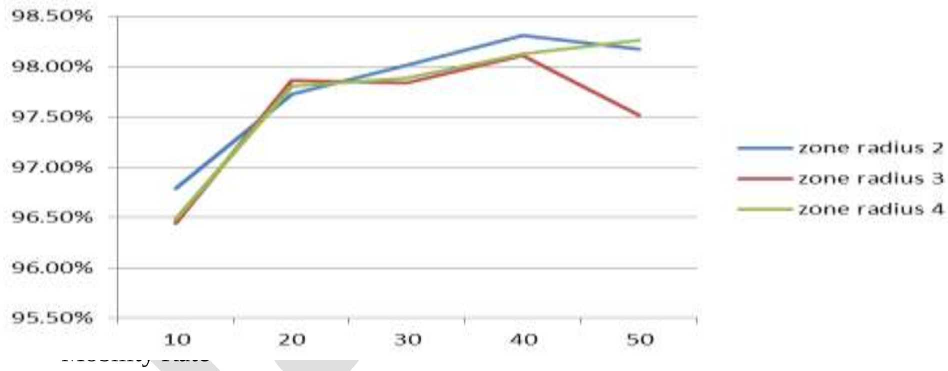


Figure 2. Mobility Rate Vs PDR

Figure 2 shows that as the zone radius increases , PDR decreases.

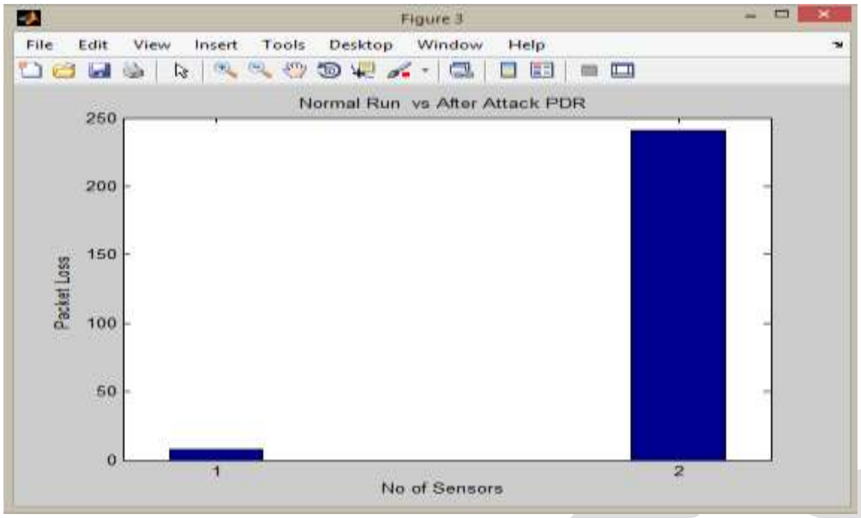


Figure 3 is also a reflection of how no. of message packets are affected when there is an attack being introduced this graph shows how many packets have been lost (control message) when there was no. of attacks and after attack

x-axis=mobility Rate

y-axis=Average Delay

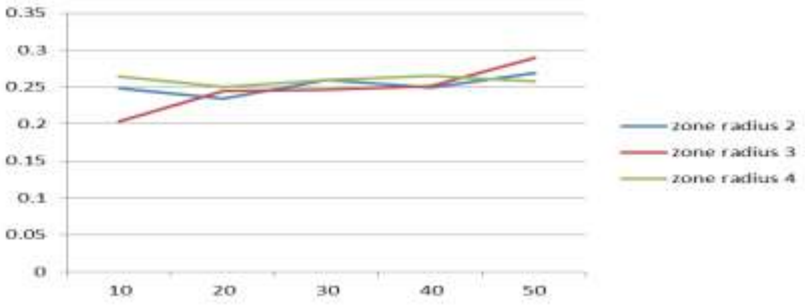
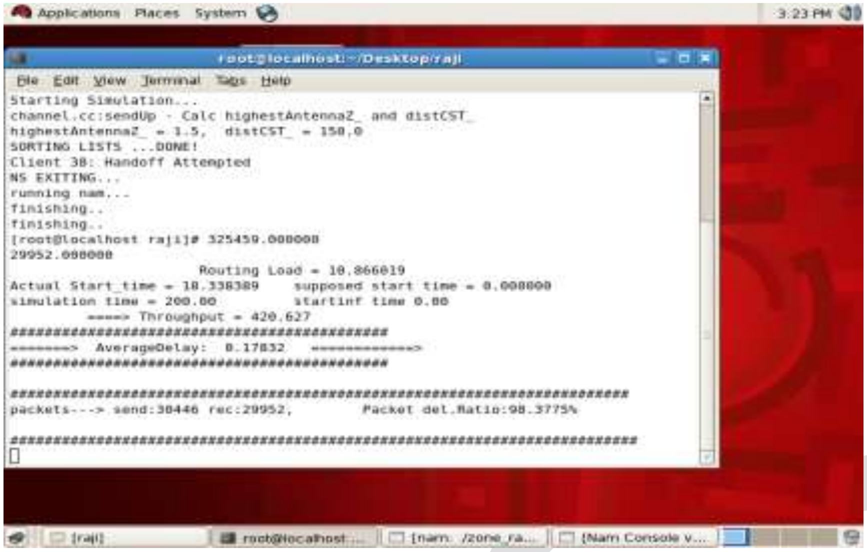


Figure 4, Mobility Vs End to End Average Delay

Figure 4 shows that the impact of mobility rate on average delay and after attack there is increase in average delay


Applications Places System
3:23 PM
root@localhost:~/Desktop/raji
File Edit View Terminal Tabs Help
[raji]
root@localhost:...
[nam: /zone_ra...
[Nam Console v...

```
Starting Simulation...
channel.cc:sendUp - Calc highestAntennaZ_ and distCST_
highestAntennaZ_ = 1.5,  distCST_ = 150.0
SORTING LISTS ...DONE!
Client 38: Handoff Attempted
NS EXITING...
running nam...
finishing..
finishing..
[root@localhost raji]# 325459.000000
29952.000000
                        Routing Load = 10.866019
Actual Start_time = 10.338389    supposed start time = 0.000000
simulation time = 200.00         startinf time 0.00
          ====> Throughput = 420.627
#############################################
=======>  AverageDelay:  0.17832   ============>
#############################################

##########################################################################
packets---> send:30446 rec:29952,        Packet del.Ratio:98.3775%

##########################################################################
```

Figure5. shows the throughput ,average delay and packet delivery ratio under zone routing protocol

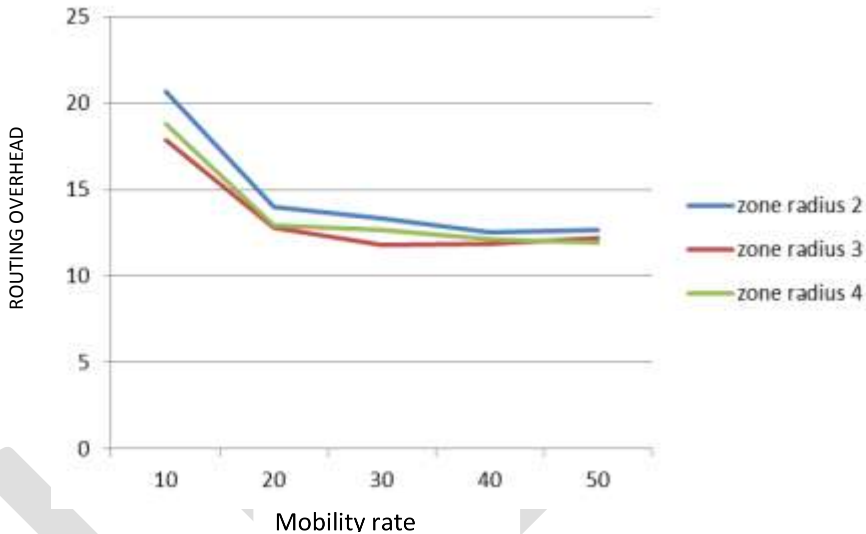


Figure 6 Mobility Rate vs Routing Overhead

6. CONCLUSION AND FUTURE SCOPE

Simulation results have shown that mobility and transmission range do have impact on zone routing protocol as zone size gets increased then delay keeps on reducing. We have considered the problem of DOS attacks in MANETS and proposed our simulated approach for security in MANETS. Our results confirm that DOS attacks can be detected easily and efficiently than the AODV based reputation protocol. In future scope of this research work we can develop a mathematical model for detection of many types of attacks.

REFERENCES:

[1] Ashish K Maurya and Dinesh Singla “Simulation based performance comparison of AODV,FSR,ZRP routing protocols in MANET”, International Journal of computer applications. Foundation of computer science 12(2), December 2013, pp 23-18.

[2] T Ravi Nayak et al. “Implementation of Adaptive Zone Routing protocol for wireless network”, International Journal of engineering Science and Technology Vol.2 (12), 2013 pp 7273-7288.

[3] Rajneesh Kumar Gujral, Manpreet Singh "Analyzing the Impact of Scalability on QoS Aware Routing for MANETs "International Journal of Computer Science MANETs vol. 8(3), pp no. 487-495, May 2013,Issue ISSN (online): 1694-0814.

[4] Preeti Arora and GN Purohit “Comaparative Analysis of Adhoc Routing Unicast Protocols(using WiMAX Environment”, IJCSI International Journal of computer science issues ,Vol-8 Issue2,March 2011.

[5] Sree Ranga Raju and Jitendranath Mungara “ Performance Evaluation of ZRP over AODV and DSR in Manet using Qualnet”, European Journal of Scientific Research ISSN 1450-216X Vol. 45 No 4(2010) pp 651-667.

[6] Md. Saiful Azad, Mohammad Moshee Uddin, Farhat Anwar and Md. Arafatur Rahman “Performance Evaluation of Wireless Routing protocols in Mobile Wimax Environment”, Proceedings of the international multiconference of engineers and computer scientists 2008, vol. 2 IMECS 2008, 19-21 March,2008 Hong Kong.

[7] Brijesh Patel and Sanjay Srivastava, “Performance Analysis of Zone Routing Protocols in Mobile Ad hoc Networks” Dhirubhai Ambani Institute of Information and Communication Technology Gandhinagar 382 007, India, 2006.

[8] Charles E.Perkins and Elizabeth M. Royer, “Ad hoc on demand distance vector (AODV) routing (Internet-Draft)”, Aug- 2013.

[9] H. Yang, et al, "SCAN: Self-Organized Network-Layer Security in Mobile Ad Hoc Networks," IEEE Network, vol. 24, 2012, pp. 1-13.

[10] Hoang Lan Nguyen, Uyen Trang Nguyen. “*A study of different types of attacks on multicast in mobile ad hoc networks”.* Ad Hoc Networks, Volume 6, Issue 1, Pages 32-46, January 2012