Proceedings of the International Conference on Man-Machine Systems (ICoMMS)
11 – 13 October 2009, Batu Ferringhi, Penang, MALAYSIA

Security and Scalability of MANET Routing Protocols in Homogeneous & Heterogeneous Networks

T.V.P. Sundararajan [1], Karthik[2] , A. Shanmugam[3]
1. Assistant Professor, Bannari Amman Institute Of Technology, Sathyamangalam
2. Student, Bannari Amman Institute Of Technology, Sathyamangalam
3. Principal, Bannari Amman Institute Of Technology, Sathyamangalam
E-mail id: tvpszen@yahoo.co.

***Abstract*- A Mobile Ad-Hoc Network (MANET) is a collection of wireless mobile nodes forming a temporary network without using any centralized access point, infrastructure, or centralized administration. During data transmission between these nodes there may be malicious threats, attacks, and penetrations which alters the performance of the system and insecure transmission. At that time of attack, Mobility of the different nodes makes the situation even more complicated. Multiple routing protocols especially for these conditions have been developed during the last years, to find optimized routes that free from attacks from a source to some destination. But they are not a perfect solution to this problem. The focus of this paper is to test routing performance of Seven different routing protocols (AODV, DSR, ANODR, DYMO,OLSR,OSPF,LANMAR)in variable network sizes with and without wormhole attack and to analyze their performance using various metrics in Homogeneous as well as in heterogeneous network. Analytical and simulation results are presented to evaluate the performance of the routing protocols by using Qualnet4.5.**

***Keywords* - Qualnet, ad hoc networks, wormhole attack, Scalability.**

I. INTRODUCTION

Mobile Ad hoc network (MANET) is a kind of wireless ad-hoc network, and is a self configuring network of mobile routers (and associated hosts) connected by wireless links the union of which form an arbitrary topology. Each node of an ad hoc network can both route and forward data. The routers are free to move randomly and organize themselves arbitrarily; thus, the network's wireless topology may change rapidly and unpredictably. Such a network may operate in a standalone fashion, or may be connected to the larger Internet.

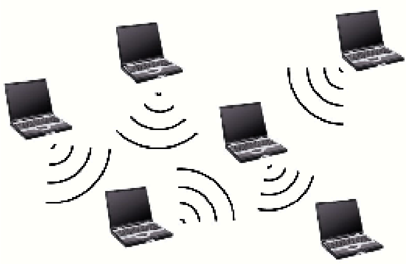


Fig.1. Mobile Ad hoc network

This paper provides a simulation study that identifies security and scalability issues and illustrates the effects of those threats on network performance when the AODV, DSR, ANODR, DYMO, OLSR, OSPF, LANMAR routing protocol were used in both homogeneous and heterogeneous networks. Also, we analyze the performance of seven different protocols in various network sizes with and without wormhole attack and we detailed our studies.

II. DESIGN OF EXPERIMENT AND CONFIGURATION SETUP

Past simulation tools lack the ability to simulate large scale networks in an accurate manner. This is due to the fact that past simulation tools require an immense amount of memory and runtime that make such studies impractical. QualNet on the other hand, is a scalable network simulation library that was designed with the primary goal of simulating large high fidelity models of wired, wireless, and mixed networks in an efficient manner. The simulations were performed with four different area sizes and numbers of nodes, 10, 20, 30 and 60 nodes in homogeneous & heterogeneous network. Heterogeneous environment is involved with WIMAX, Zigbee, wired network and wi-fi. .In order to analyze like a real environment we created a scenario where the nodes were randomly distributed with different subnets.

III. SIMULATION ENVIRONMENT

The simulations were performed using the Qualnet Simulator v4.5 from Scalable Network Technologies.

A. Simulation speed and scalability

Although Scalable Networks describes QualNet Simulator as very fast and scalable and supporting 10‟s of thousands of nodes, we were not able to run all simulations initially planned for this project. At first we intended to employ 1000 nodes, as this number was often chosen in other papers. Unfortunately, we realized that the simulation is not feasible at this number of nodes, because it would require huge system resources and take weeks to complete [1]. As the university edition of QualNet only supports sequential execution on one processor. So we decided to re-dimension the project to 60 nodes.

IV. AD-HOC NETWORK ROUTING PROTOCOLS

A. Ad Hoc On-Demand Distance Vector Routing (AODV)

The Ad Hoc On-Demand Distance Vector routing protocol (AODV) is an improvement of the Destination-

Sequenced Distance Vector routing protocol (DSDV). The Ad Hoc on Demand Distance Vector (AODV) routing protocol provides unicast, broadcast and multicast communications in ad hoc mobile networks. It is an on demand algorithm, i.e., it searches for routes between nodes only as desired by source nodes; these routes are maintained as long as they are needed by the sources [2].

B. Dynamic Source routing protocol (DSR)

DSR is a simple and efficient routing protocol that facilitates load balancing by allowing multiple routes to any destination .DSR employs explicit source routing. All the packets carry a list of intermediary nodes that they should pass through from the sender to the destination. The source is able to select an ideal path amongst a set of available routes [2]. When a source S needs to send data packets to a destination D, S first checks its local cache to determine if it has an available path to D. Piggybacking is used to prevent infinite recursion of route discovery & more secured data transfers are its advantages.

C. Anonymous on Demand Routing protocol (ANODR)

The route pseudonymity approach allows mobile nodes to transmit their packets anonymously without identifying the sender and the receiver. ANODR avoids using public key cryptosystems if symmetric key cryptosystems can provide the needed support. It also avoids using symmetric key cryptosystems if not indispensable. Onion is a cryptographic onion that is critical for route pseudonym establishment.. One limitation of ANODR is the sensitivity to terminal node mobility. As nodes move, the path is broken and must be reestablished. To enhance performance in a mobile environment, and in particular to mitigate the disruption caused by path breakage, we can use multiple paths. Sequential path computation has the advantage of allowing online maintenance—if a path fails, a new path is computed while the remaining paths are still in use.

D. Dynamic MANET On-demand routing protocol (DYMO)

The Dynamic MANET On-demand (DYMO) routing protocol enables reactive, multi-hop unicast routing between participating DYMO routers. In order to react to changes in the network topology, DYMO routers monitor links over which traffic is flowing. When a data packet is received for forwarding and a route for the destination is not known or the route is broken, then the DYMO router of source of the packet is notified. A Route Error (RERR) is sent toward the packet source to indicate the current route to a particular destination is invalid or missing. When the source's DYMO router receives the RERR, it deletes the route. DYMO uses sequence numbers to avoid use of stale routing information.

E. Optimized link state routing protocol (OLSR)

The protocol inherits the stability of a link state algorithm and has the advantage of having routes immediately available when needed due to its proactive nature. OLSR minimizes the overhead from flooding of control traffic by using only selected nodes, called MPRs (Multi Point Relays), to retransmit control messages. This technique significantly reduces the number of retransmissions required to flood a message to all nodes in the network. Secondly, OLSR requires only partial link state to be flooded in order to provide shortest path routes. OLSR may optimize the reactivity to topological changes by reducing the maximum time interval for periodic control message transmission. Furthermore, as OLSR continuously maintains routes to all destinations in the network, the protocol is beneficial for traffic patterns where a large subset of nodes are communicating with another large subset of nodes, and where the [source, destination] pairs are changing over time.

F. Landmark ad hoc routing protocol (LANMAR)

The Landmark Ad-hoc Routing Protocol (LANMAR) is designed to dramatically reduce routing table size and routing update overhead in large-scale ad-hoc networks that exhibit group mobility. LANMAR combines the features of Fisheye State Routing (FSR) and landmark routing; this added some features like landmark election to cope with the dynamic and mobile environment. Other advantages of LANMAR include the use of landmarks for each logical group in order to reduce routing update overhead, and the exchange of ”scoped” link state with neighbors only. By virtue of land marking, remote groups of nodes are “summarized by the corresponding landmarks. As a result, each node still maintains accurate routing information about immediate neighborhood; at the same time it will keep track of the routing directions to the landmarks nodes, and thus, to remote group.

G. Open shortest path first (OSPF)

Open Shortest Path First (OSPF) is a recent entry into the Internet interior routing scene. OSPF is a link-state routing protocol with a complex set of options and features. Some of the advantages of these routing protocols are Scalability, Full sub netting support, Type of Service.

V. ACTIVE ATTACK

A. Wormhole attack

Active attacks, involve intruders altering the victim’s network state. A wormhole attack is an example of an active attack. In a wormhole, the attacker creates an artificially fast shortcut in the network to bias route discovery. The two ends of a wormhole break network and routing rules, notifying the rest of the network that all packets were received, and super fast. A wormhole link then appears as a high bandwidth and low latency path. “Smart” routing protocols note this fast route and start sending all the network control flow traffic through this “high performance” link. Once the adversarial node is in the network’s critical path, the wormhole relays all control traffic but drops all, or most, data. Wormholes can distinguish between control flow and data flow based on packet length, transmission timing, broadcast /unicast packet types etc. A wormhole circumvents any secure cryptographic scheme as well, because its goal is not to steal the data, but instead drop data and severely disrupt the network. An example of a protective measure that is useless against wormholes is a cryptographic checksum. Under this scheme, the network detects inauthentic packets forged by an active attacker when packets have incorrect checksums, i.e., the length of the packet is not equal to the checksum it was sent with. But this cannot stop wormholes, because the packets relayed by wormholes are all valid with proper crypto checksums [3]. In mobile wireless environments, it is hard to distinguish between malicious packet loss by the likes of a wormhole from environmental loss such as those due to mobility and wireless interference, etc.

V. MOBILITY MODEL

An important factor in mobile ad-hoc networks is the movement of nodes, which is characterized by Speed, direction and rate of change.

A. Random way point model

In this model, a mobile node moves from its current location to a randomly chosen new location within the simulation area, using a random speed uniformly distributed between [Vmin, Vmax]. Vmin refers to the minimum speed of the simulation, Vmax to the maximum speed [5]. The Random Waypoint Mobility Model includes pause times when a new direction and speed is selected. As soon as a mobile node arrives at the new destination, it pauses for a selected time period (pause time) before starting traveling again.

VI. PERFORMANCE ANALYSIS METRICS

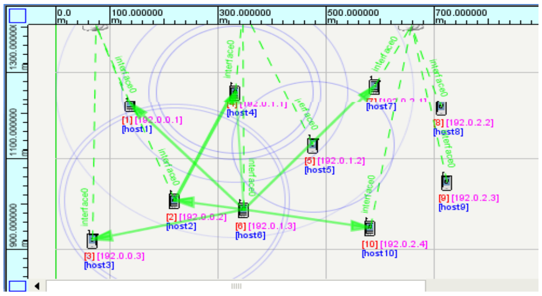
•*Packet delivery ratio (PDR):* Packet delivery ratio is calculated by dividing the number of packets received by the destination through the number of packets originated by the application layer of the source (i.e. CBR source). It specifies the packet loss rate, which limits the maximum throughput of the network. The better the delivery ratio, the more complete and correct is the routing protocol

•*Average End-to-end delay (AED):* End-to-end delay indicates how long it took for a packet to travel from the CBR source to the application layer of the destination. It represents the average data delay an application or a user experiences when transmitting data.
We group AODV, DSR, ANODR, and DYMO protocols in on demand routing protocol and remaining OLSR, OSPF & LANMAR in other routing protocol.

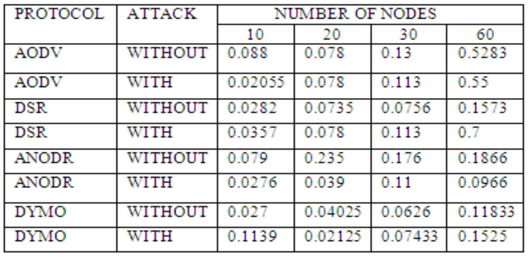
A. Parameter settings for scenario without attack:

NODE SIZE	10,20,30,60
ATTACK	NIL
MOBILITY	RANDOM WAY POINT
NODE PLACEMENTS	RANDOM
PROTOCOL	AODV,DSR,ANODR,OSPF DYMO,OLSR,LANMAR,
PAUSE TIME	30ms
MAX PAUSE TIME	10ms
MIN PAUSE TIME	0ms

B. Animated Scenario:

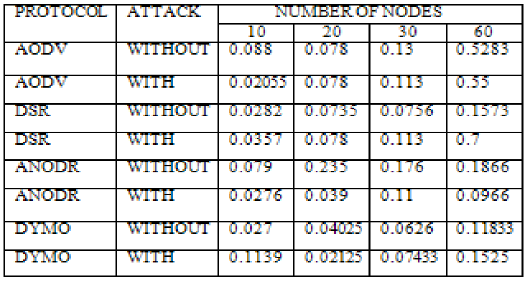


C. Simulation results of on demand routing protocols in homogeneous network without attack for PDR:



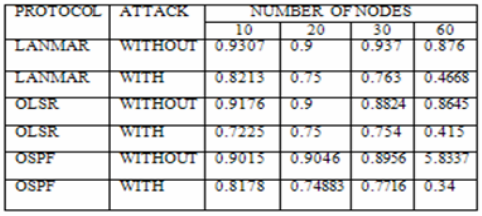
PROTOCOL	ATTACK	NUMBER OF NODES			
		10	20	30	60
AODV	WITHOUT	0.088	0.078	0.13	0.5283
AODV	WITH	0.02055	0.078	0.113	0.55
DSR	WITHOUT	0.0282	0.0735	0.0756	0.1573
DSR	WITH	0.0357	0.078	0.113	0.7
ANODR	WITHOUT	0.079	0.235	0.176	0.1866
ANODR	WITH	0.0276	0.039	0.11	0.0966
DYMO	WITHOUT	0.027	0.04025	0.0626	0.11833
DYMO	WITH	0.1139	0.02125	0.07433	0.1525

D. Simulation result for on demand routing protocols without attack for AED:



PROTOCOL	ATTACK	NUMBER OF NODES			
		10	20	30	60
AODV	WITHOUT	0.088	0.078	0.13	0.5283
AODV	WITH	0.02055	0.078	0.113	0.55
DSR	WITHOUT	0.0282	0.0735	0.0756	0.1573
DSR	WITH	0.0357	0.078	0.113	0.7
ANODR	WITHOUT	0.079	0.235	0.176	0.1866
ANODR	WITH	0.0276	0.039	0.11	0.0966
DYMO	WITHOUT	0.027	0.04025	0.0626	0.11833
DYMO	WITH	0.1139	0.02125	0.07433	0.1525

E. Parameter settings for scenario with attack:



PROTOCOL	ATTACK	NUMBER OF NODES			
		10	20	30	60
LANMAR	WITHOUT	0.9307	0.9	0.937	0.876
LANMAR	WITH	0.8213	0.75	0.763	0.4668
OLSR	WITHOUT	0.9176	0.9	0.8824	0.8645
OLSR	WITH	0.7225	0.75	0.754	0.415
OSPF	WITHOUT	0.9015	0.9046	0.8956	5.8337
OSPF	WITH	0.8178	0.74883	0.7716	0.34

F. Simulation results of other routing protocols in homogeneous network with attack for PDR:

ATTACK	WORMHOLE
MAC PROTOCOL	WORMHOLE
WORMHOLE TUNNELING BANDWIDTH	10000000

G. Simulation results of other routing protocols in homogeneous network with attack for AED:

PROTOCOL	ATTACK	NUMBER OF NODES

[redacted]

PROTOCOL	ATTACK	NUMBER OF NODES			
		10	20	30	60
AODV	WITHOUT	0.6882	0.74005	0.96122	0.90521
AODV	WITH	0.364	0.50315	0.41363	0.48043
ANODR	WITHOUT	0.5454	0.5746	0.65	0.5427
ANODR	WITH	0.18279	0.3837	0.25748	0.19428
DYMO	WITHOUT	0.6385	0.6868	1.1407	3.783
DYMO	WITH	0.2759	0.4371	0.3389	0.3915

I. Simulation results of on demand routing protocols in heterogeneous network without attack for AED:

PROTOCOL	ATTACK	NUMBER OF NODES			
		10	20	30	60
AODV	WITHOUT	0.00504	0.01195	0.011033	0.0405
AODV	WITH	0.00081	0.006905	0.005033	0.0043
ANODR	WITHOUT	0.0051	0.00975	0.00966	0.00966
ANODR	WITH	0.00035	0.0047	0.00593	0.0035
DYMO	WITHOUT	0.0068	0.01325	0.00336	0..0027
DYMO	WITH	0.00109	0.0051	0.00633	0.00441

J. Simulation results of other routing protocols in heterogeneous network with attack for PDR:

PROTOCOL	ATTACK	NUMBER OF NODES			
		10	20	30	60
LANMAR	WITHOUT	0.638	0.6153	0.752	0.9679
LANMAR	WITH	0.2737	0.4615	0.3565	0.40112
OLSR	WITHOUT	0.6385	0.6167	0.7944	0.74436
OLSR	WITH	0.2759	0.4366	0.3573	0.39336
OSPF	WITHOUT	0.6609	0.6226	0.8287	0.71383
OSPF	WITH	0.2802	0.4656	0.3564	0.71383

K. Simulation results of other routing protocols in heterogeneous network with attack for AED

PROTOCOL	ATTACK	NUMBER OF NODES			
		10	20	30	60
LANMAR	WITHOUT	0.0042	0.0045	0.0085	0.00139
LANMAR	WITH	0.00029	0.00345	0.3565	0.00313
OLSR	WITHOUT	0.00394	0.01022	0.01098	0.0142
OLSR	WITH	0.00029	0.003645	0.0037	0.00178
OSPF	WITHOUT	0.00396	0.00535	0.009066	0.0092
OSPF	WITH	0.00029	0.0029	0.004633	0.713833

VII. ANALYZING THE RESULTS FOR HOMOGENEOUS NETWORKS FOR PDR

A. On demand routing protocols with &without attack

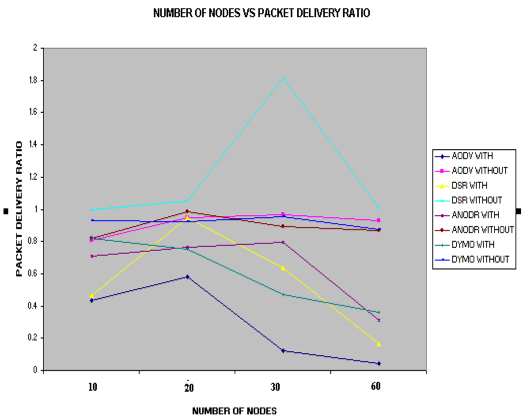


Fig.2. Analyzing graph for on demand routing protocols in homogeneous networks for PDR

From fig.2.,it is clearly known that DSR performs well in delivering the packets when there is no attack. Due to the random mobility, the nodes which are in the intermediate hop will perform the broadcast based searching process until the packets are delivered. So, at the maximum the packets get delivered. When the nodes get increased the number of intermediate hop also gets increased. So, many routes are possible at that time. So packet delivery ratio gets decreased since same data rate packets are sent to the large number of nodes. When attack takes place in large number of nodes, the intermediate hop gets varied which leads to decrease in PDR since packets drops invariably. DYMO is performing well in large scale scenario with attack because it uses Sequence number for Route Discovery which eliminates the Stale routing information.

B. Other routing protocols with &without attack

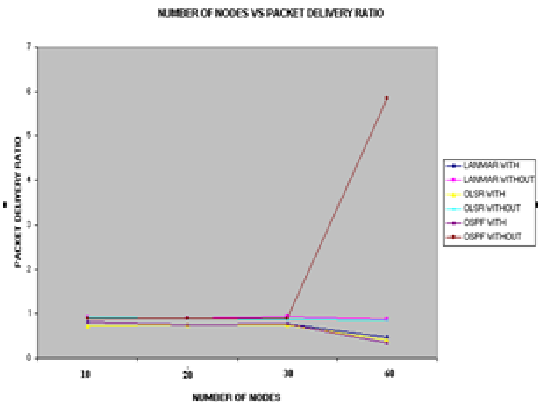


Fig.3. Analyzing graph for other routing protocols in homogeneous networks for PDR

Fig.3. shows that OSPF performs well when there is no attack because the protocol is especially designed for the purpose of supporting the subnets and mainly for scalability. After 30 nodes PDR is drastically increasing because TOS maintains the avoidance of delay which mutually leads to increase of PDR. But when we introduce the attack LANMAR performs well because it is designed to cope up with dynamically changing environment and also mainly to reduce the routing table size along with Land marking which leads to update the routes accurately even there is any attack.

VIII. ANALYZING THE RESULTS FOR HOMOGENEOUS NETWORKS FOR AED

A. On demand routing protocols with & without attack

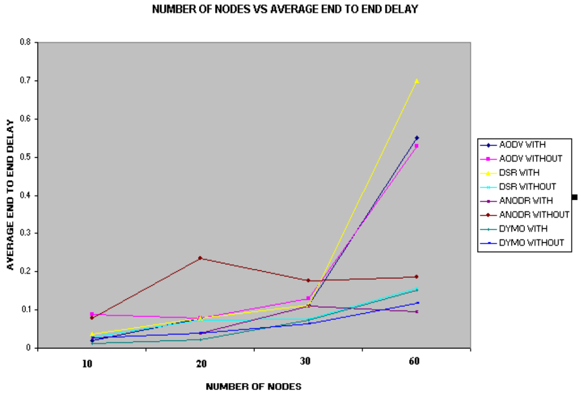


Fig.4. Analyzing graph for on demand routing protocols in homogeneous networks for AED

From fig 4, it is known that DYMO have little amount of End to end delay. In DYMO, when the originator's DYMO router receives the RREP, routes have then been established between the originating DYMO router and the target DYMO router in both directions. So, AED get decreased But the delay is increasing when we increase the nodes because when the node size increases their throughput reduces so that its AED increases. After introducing the attack it seems that in ANODR performs well for small scale because of employing special features for anonymous transfer of packets. But when we introduce the attack with increase in the number of nodes Sequential path computation did the on - line maintenance of route if there occurs any errors. Mechanism of delivering the packets, i.e. it drops the Packets invariably when there is attack.

B. Other routing protocols with & without attack

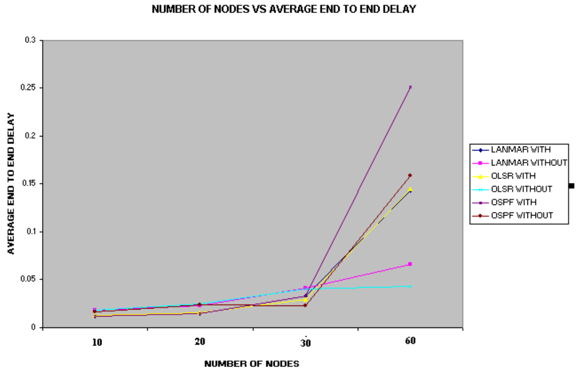


Fig.5. Analyzing graph for other routing protocols in homogeneous networks for AED

From fig 5, it is clearly understood that when there is no attack OLSR Performs well because OLSR is well suited for networks, where the traffic is random and sporadic between a larger set of nodes rather than being almost exclusively between a small specific set of nodes. Along with it OLSR minimizes the overhead from flooding of control traffic by using only selected nodes, called MPRs (Multi Point Relays), to retransmit control messages which automatically reduce the average end to end delay. Up to 30 nodes OSPF have only less AED this is because of Type of Service that avoids delay but it is to some extent of nodes. When we introduce attack LANMAR Performs because it has LANMAR-neighbor-timeout-interval that controls how fast node can detect link failures, by this the link it identify the errors which leads to less AED when compared with other routing protocol while there exist attack.

IX. ANALYZING THE RESULTS FOR HETEROGENEOUS NETWORKS FOR PDR

A. On demand routing protocols with & without attack

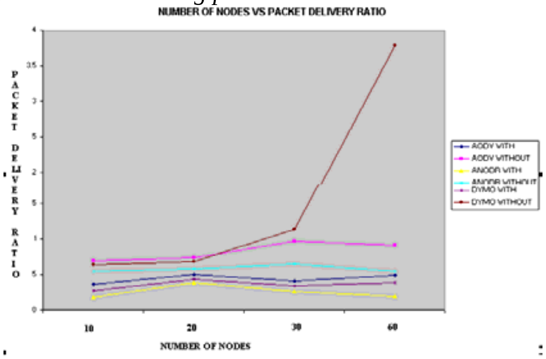


Fig .6. Analyzing graph for on demand routing protocols in heterogeneous networks for PDR

From fig.6, it is evident that when there is no attack DYMO performs well in large scale networks. This is because in order to react to changes in the network topology, DYMO routers monitor the links which includes the interfaces over which traffic is flowing. Because of this PDR drastically get increased. When we introduce an attack it is vividly known that AODV performs well. This is because the remaining protocols have some additive features which tend to reduce the packets when they are moving in different interfaces hence their hop counts and the intermediate hop counts get varied. It is not happening in AODV because it mutually supporting different interfaces.

B. Other routing protocols with & without attack

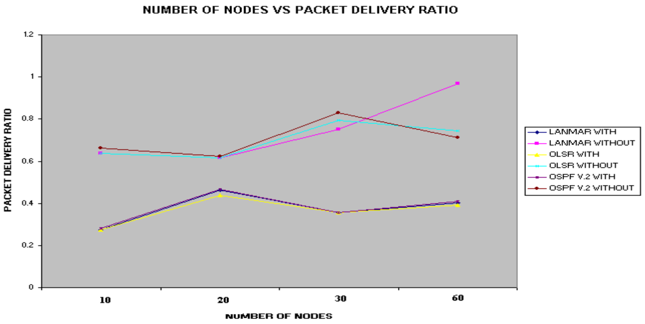


Fig .7. Analyzing graph for other routing protocols in heterogeneous networks for PDR

From fig.7, it is known that when there is no attack LANMAR performs well because it is basically designed to large scale scenario with increased throughput and low delay. Even though attack is introduced LANMAR performed well because of Land marking technique which reduces the routing table size and accurately updates the routing information.

X. ANALYZING THE RESULTS FOR HETEROGENEOUS NETWORKS FOR AED

A. On demand routing protocols with & without attack

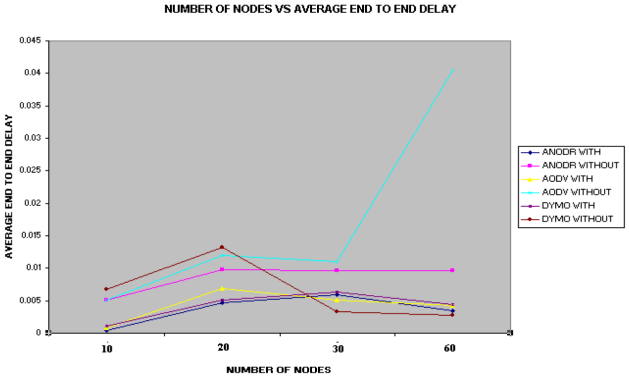


Fig .8. Analyzing graph for on demand routing protocols in heterogeneous networks for AED

Fig .8 shows that when there is no attack in DYMO performs well. For PDR also DYMO performs well when there is no attack. This is because when the packets are successfully sent, normally AED is preferably gets reduced. When there is an attack in DYMO the ADE get increased to a great extent for small number of nodes. While node number gets increased AODV performs well in a normal way as like that in PDR.

B. Other routing protocols with & without attack

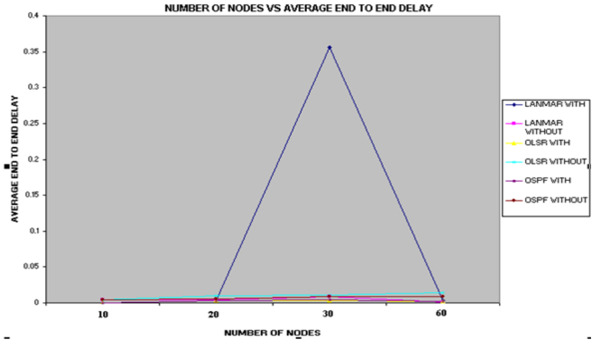


Fig .9. Analyzing graph for other routing protocols in heterogeneous networks for AED

From the fig 9, OLSR performs well when there is no attack. It employs effective transfer of packet without more amount of delay. While the network size increases the AED get decreased. This is because of the use of Multi Point Relays. When there is an attack OSPF performs well because this is the recently designed protocol which supports Subnetting and mainly for scalability. In addition to it TOS is used in order to reduce the delay.

XI. CONCLUSION

In this paper, first we have made a performance comparison of seven different mobile ad-hoc routing protocols with respect to various network sizes in homogeneous and heterogeneous network. In the next level, we test the performance of same protocols in the presence of attacking nodes. In previous works performance of routing protocols were evaluated as function of mobility rate and speed without considering the network size. However Scalability is a very important factor in some applications of mobile ad-hoc networks (e.g. WSN), as it determines if a protocol will function or fail when the number of mobile users increases. We used QualNet simulator, which is commercial and said to be faster than ns-2 for instance. However, the simulation speed is still slow and we were only able to perform a single run per scenario in the context of this project. Therefore, those results should be validated through multiple, additional simulation runs in a future work.

The performances of all the discussed protocols were decreased because huge amount of system resources and processing power needed when network size increases. In homogeneous networks among on demand routing protocols DYMO performs 21.5% well. Among other protocols LANMAR performs 12.9% well. In heterogeneous networks among on demand routing protocols DYMO performs about 18.4% well. Among other protocols LANMAR is performing 9.4% well. When there is an attack overall performance reduced about 20.1%.The packet delivery ratio in homogeneous network was 33% greater than homogeneous networks because in homogeneous network there is no different devices, no different frequencies and no different interfaces needed hence packet delivery ratio is more. The average end to end delay in heterogeneous network is greater than homogeneous network by 8%.

XII. FUTURE WORK

We would like to extend our work with some other performance metrics like hop counts, tunneling ratio along with different mobility models with different pause time in large scale networks. Our future goal is to learn how protocol parameters such as thresholds should be set. Given these parameters we will determine how many friends per benign node are needed to tolerate a given percentage of malicious nodes. We will also investigate how to incorporate security solutions against above discussed attack. Also, performance analysis of routing protocols in the emulation environment is of interest as well.

REFERENCES

[1] Sheeraz Ahmed,Muhammad Bhilal,Umer Farooq, FazleHadi(2007), “Performance Analysis of various routing strategies in Mobile Ad hoc Network using QualNet simulator”, IEEE,1-6,2007.

[2] David oliver jorg(2003)“Performance comparison of MANET Routing Protocols in different environment”,IEEE,1-6,2003

[3] Scalable Network Technologies, "Qualnet simulator",Software Package, 2003[Online]. http://www.scalable-networks.com

[4] Julian Hsu, Sameer Bhatia, Ken Tang, Rajive Bagrodia, Michael J. Acriche, ” Performance of Mobile Ad-Hoc Networking Routing Protocols in Large Scale Scenarios”, pp. 1-7, 2004.

[5]]Arun Kumar B.R, Lokanatha C.Reddy, Prakash S.Hiremath, ”Performance Comparison of Wireless Mobile Ad-Hoc Network Routing Protocols”, IJCSNS International Journal of Computer Science and Network Security, VOL.8 No.6, pp. 337-343, June 2008.