Analysis of MANET's Routing Protocols, Security Attacks and Detection Techniques- A Review

Amina Yaqoob, Alma Shamas, Jawwad Ibrahim
Aminayaqoob9@gmail.com arfa.noor91@gmail.com sultan.zia@cs.uol.edu.pk

Department of Computer Science and Information Technology, University of Lahore, Gujrat Campus
Department of Computer Science and Information Technology, University of Lahore, Gujrat Campus
Department of Computer Science and Information Technology, University of Lahore, Gujrat Campus

Abstract
Mobile Ad hoc Network is a network of multiple wireless nodes which communicate and exchange information together without any fixed and centralized infrastructure. The core objective for the development of MANET is to provide movability, portability and extensibility. Due to infrastructure less network topology of the network changes frequently this causes many challenges for designing routing algorithms. Many routing protocols for MANET have been suggested for last few years and research is still going on. In this paper we review three main routing protocols namely Proactive, Reactive and Hybrid, performance comparison of Proactive such as DSDV, Reactive as AODV, DSR, TORA and Hybrid as ZRP in different network scenarios including dynamic network size, changing number of nodes, changing movability of nodes, in high movability and denser network and low movability and low traffic. This paper analyzes these scenarios on the performance evaluation metrics e.g. Throughput, Packet Delivery Ratio (PDR), Normalized Routing Load(NRL) and End To-End delay(ETE).This paper also reviews various network layer security attacks challenge by routing protocols, detection mechanism proposes to detect these attacks and compare performance of these attacks on evaluation metrics such as Routing Overhead, Transmission Delay and packet drop rates.

Keywords:
Routing Protocols, DSDV, AODV, DSR, TORA, ZRP, Security Attacks, Detection Techniques

1. Introduction:

Ad Hoc networks are well known and useful because of infrastructure less nature. Wireless network is a group of hubs, in this network nodes corporate with each other by forwarding packets and permit nodes to communicate with others. All nodes in MANET[1] move randomly towards any path, due to this it connects to different devices as often as possible. Design an architecture for MANET is a complicated task cause of dynamic nature of MANET. Various routing protocols have been designed to accomplish this task. Routing is a way of picking optimal route to exchange the data packets from intended source to adjacent nodes to destination node over the network. "MANET" routing protocols are a baseline that controls the movement of data packets within the network and determines which route must be chased through the data packs to arrive at the end point. In ad-hoc network, network topology isn't secure due to nodes mobility. As a result, we don't have a fixed way to start with one hub then onto the next hub in the system, they need to find by the declaration of its quality. Each hub in the system must tune in to declarations communicated through their adjacent hubs.[2] MANET protocols can be listed in to three broad categories which are: "Proactive or Table driven[3]", "Reactive or On-request[4]" and "Hybrid". Once a device enters the network or switches its location, routes to a destination is defined through proactive routing protocols, which are managed by periodic path updates.

Routes are discovered as required in reactive routing protocols, which are destroyed after a specific time. While hybrid routing protocols have features of Reactive and Proactive routing protocols to better cope in varying networks size and varying nodes movability [5]. Implementing routing functions needs memory, calculation power, anyway cell phones include physical size and weight restrictions basic for their movability. Security of manet is another issue. Due to the movement of nodes intruders can enter into the network. To ensure the secure communication between the node's communication links are required. Connection of a node should be powerful enough to recognize other node before creating reliable connection. As a consequence, node requires to supply other nodes its name as well as related credentials. However, the transmitted identity and credentials need to be authenticated and secured such that receiver node cannot doubt the validity and reliability of the transmitted identity and credentials. To ensure ad hoc networking, therefore, it is important to have a security infrastructure[6].In this paper we will review routing protocols, routing protocols' comparison[7][8]in various network scenarios, security attacks and measures to detect these attacks. Section 3 provides classification and review of routing protocols, section 4 reviews performance

Manuscript received June 5, 2024
Manuscript revised June 20, 2024
https://doi.org/10.22937/IJCSNS.2024.24.6.4

evaluation metrics, section 5 reviews performance comparison of protocols in different network scenarios. Section 6 reviews security attack and detection techniques.

2. Classification of routing protocols:

Routing protocols used to manage the movement of data and identified which route should a packet select to transmit data from intended node to destination node. In this paper we study Routing protocols in MANET classified into three types based on their routing tactics[3].

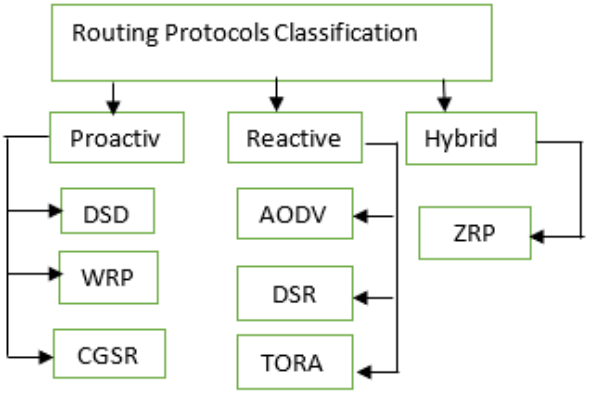


Fig1.Classification of routing protocols

2.1 Proactive Routing Protocols: These are named as table driven[3] which means every node requires to maintain a table that comprises uniform and timely routing information before a node start its communication. Some popular Proactive routing protocols review in this paper are as follow.

1. Destination sequence distance vector routing (DSDV)
2. Wireless routing protocol (WRP)
3. Cluster Gateway Switch Routing protocol (CGSR)

2.2 Reactive Routing Protocols:

These protocols termed as on demand routing protocol which means a path is established only when requires and expires after certain time.

1. Ad hoc-on demand distance vector routing (AODV)
2. Dynamic source routing (DSR)
3. Temporarily ordered routing algorithm (TORA)

2.3 Hybrid Routing protocols:

Contains characteristics of proactive as well reactive routing protocols and scalable for large sized networks.

1. Zone Routing Protocol (ZRP)

3. Review of MANET' Routing Protocols:

I. Destination Sequence Distance Vector Routing (DSDV)

DSDV is a table-driven routing protocol, a routing table manages by all node consists of entries of all nodes in the entire network. DSDV[9] uses Bellman Ford Algorithm to find the smallest path with minimum cost from sink node to destination thus reduces routing overhead in the network. Each table entries contains information about source, next hop, sequence number and destination thus in case of a node added, remove, or a link failure occur and topology of the network changes then a broadcast sent to the entire network and nodes are periodically updated their routing tables.

II. Wireless routing protocol:

A table-driven routing protocol which is founded on distance vector routing, WRP[10] associate to family of shortest path finding algorithms. This protocol relies on Distributed Bellman ford Algorithm[11]. A routing node have information about the length of smallest path to its each adjacent to every destination and hence it is used to calculate the shortest path and each successor node along each network destination. This protocol ensures the acknowledgement process, in which each node aware of the existence of every adjacent nodes in the network through an acknowledgement receive from its neighbouring node, and if there is no message shown in the network then source node must propagate the Hello message in the network before initiate the require route.

III. Cluster Gateway Switch Routing protocol (CGSR)

CSGR[12] is hierarchal based routing, in which the entire network divides into three main entities these are termed as clusters, cluster head and a gateway. Routing in the network is done by using Least Cluster Head Change Algorithm. A node that be a part of more than one cluster is selected as a cluster gateway that provides the connection between clusters, data packets travel through one cluster head gateway to another cluster head gateway among source to destination node. each cluster has a Cluster Head, LCC algorithm used to select the cluster head which is elected only if every node has one hop distance from cluster node. Each node of the network cluster maintains only two tables namely as member table

that holds information of cluster head for every mobile node and other is routing table that holds only one record for all the nodes in that cluster.

IV. Ad hoc-on demand distance vector routing (AODV)

It is an on-demand routing protocol, it is an improved form of DSDV routing. It reduces unnecessary broadcast traffic by only establishes the routes on demand or when. The entire routing process involves two stages Route discovery and route maintenance. Route discovery is initiated by a node who requires to exchange data with other nodes, a node sent RREQ, to adjacent nodes, if intermediate node does not have path to destination, then broadcast packet to neighboring nodes, this process is repeated until route to destination is obtained. Every node in that path contains their temporary routing table include information about the source address, sequence number and destination IP address. RREP need this information in order to establish an invert path from destination to source node. In route maintenance RERR broadcast send when a broken connection detected in the network in order to discard the broken link and discover new routing path.

V. Dynamic source routing (DSR):

It is a reactive routing protocol, in DSR[13] mobile nodes able to discover a source route across several network nodes to any destination. Every mobile node keeps a route cache which holds information of recently updated routes. This protocol divided into two stages Route Discovery which occur when a mobile node requires to interconnect by other nodes in network, it first looks up it route cache if it previously has a route to destination, then it uses that route to reach to destination. And if no route available it propagates a route request (RREQ) message, each in-between node checks this broadcast to know it has information about destination, this process continuously repeated until it reaches to destination. And finally, route reply (RREP) sent by the destination or middle nodes which know the paths towards destination.

VI. Temporary ordered routing algorithm (TORA)

TORA is an on-demand routing protocol, Tora provides multiple routes from source to any destination node. It is highly adaptable, multihop routing algorithm and works on the idea of Link Reversal. The working of this protocol divided into three phases, namely as, route creation, route maintenance and route eraser. This protocol uses height constraint to examine the path of links among any node to a specified destination. A node to communicate in the network send a QUERY packet to its adjacent node, this packets continuously broadcast in the entire network until a destination node received it, or a node that knows the path to the destination. Upon receiving a QUERY, the node propagates an UPDATE packet which has its height parameter corresponding to destination, every node that obtains an UPDATE increment its height by a value than node from which the UPDATE packet obtained. Thus, this creates a directed acyclic graph form the source which propagate QUERY to the node which produced UPDATE packet.in case of adjacent node has no limited height corresponding to destination, the node discovers new routes to destination. If a network link failure detected by a node it creates a CLEAR packet to alter the routing in network.

VII. Zone Routing Protocol

It is a hybrid routing protocol[14] contains the feature of both proactive and reactive routing protocol. It acts as a proactive to discover adjacent nodes for a particular source, or acts as reactive protocol for routing between adjacent nodes. this protocol splits the whole network into several zones of dynamic size. A single node may belong to one or more overlaying zones. Size of zone defined by a total number of nodes exist in that particular zone. A zone consists of two types of nodes peripheral nodes which are placed at the edge of the zone and interior nodes which are positioned inside the zone boundary. Radius of a particular routing node specifies its distance from other nodes in a zone. IARP and IERP used by the ZRP to enhance the feature of routing in mobile ad hoc network. The node which start to communicate first lookup whether the destination node exist in its zone, if in same zone then start routes packet to destination using proactive routing protocol as Intra Zone Routing Protocol. On other hand if destination is not in same zone then source node sends QUERY packet to its peripheral nodes, nodes which have the radius or distance equals to source node. These peripheral nodes check whether the destination in their zone, and then intermediate node which knows the route to destination forward QUERY packets to destination node.

4. Performance Evaluation Metrics

To determine which MANET routing protocol performs best essential quantitative measures must be taken. various quantitative measures taken to differentiate the effectiveness of each routing protocols.[15],[16]

Packet Delivery ratio: It the ratio between numbers of data packets successfully received by the destination to the numbers of data packets sent by the source node.

$$\text{PDR} = \frac{\text{No. of Packets received}}{\text{No. of packets sent}} \text{X } 100 \qquad (1)$$

Average End-to-End Delay: It is the time taken by a data packet to travel from source node to destination.it includes all the possible delays that can occur in network including packets queuing delay, transmission delays, signalling delays. It is calculated as sum of all packets received by destination node to the total number of packets sent by source.

$$\text{ETE} = \frac{\Sigma\, sent_{time} - \Sigma\ \text{Received\_time}}{\text{N}} \qquad (2)$$

Sent_time is the total time of packet send by source to destination, receive_time is the total time packet delivered to destination, number of packets transferred on constant bit rate in the network denoted by N.

Throughput: It identifies number of packets transmitted to destination in particular period of time.

$$\text{Throughput} = \frac{\text{packets received}}{\text{transmission time}} \qquad (3)$$

Normalized Routing Load: It is ratio of number of data packets transmitted to the total number of packets received.

$$\text{NRL} = \frac{total\ \ routing\ packets\ transmitted}{total\ packets\ received} \qquad (4)$$

5. Comparison of evaluation metrics on routing protocols:

In order to obtain numerical calculations through performance metrics, Network Simulator(NS2)[17] proposed in this paper. traffic generated by the network using constant Bit Rate (CBR). every time source CBR sent UDP packets, and size of each packet remains constant that is 512 bits. Random Waypoint Model proposed to determine the mobility of nodes in network. To assess the performance of routing protocols two scenarios are taken.[18][19].

1. Impact of low movability of nodes in low traffic networks.
2. Impact of high movability, or changing number of nodes.

5.1 Impact of Throughput in low movability of nodes and in low traffic networks

Movability of nodes termed as speed of nodes, As the speed of nodes changing gradually, it directly effects the evaluation metrics e.g. NRL, ETE delay, throughput, PDF.

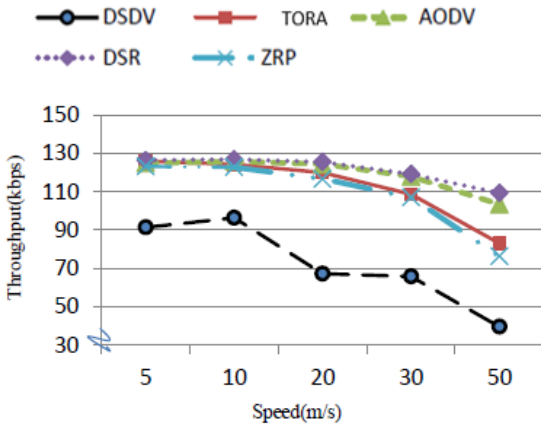


Fig. 1 Throughput Vs. Mobility.

From fig 1 we can see speed of nodes gradually increases from 5ms-1 to 25ms-1 with number of nodes 25. All protocols exhibit the same performance when the movability of nodes slow, but as the speed of nodes increases throughput of DSDV becomes worse, AODV, TORA and DSR perform better in low mobility and low traffic, ZRP approximately has high throughput than DSDV.

5.2 Impact of PDF in low movability of nodes and in low congestion network

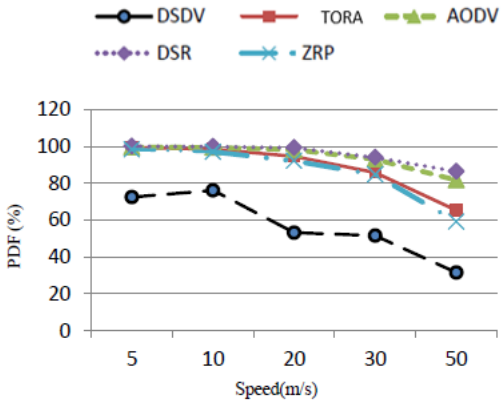


Fig. 2 PDF Vs. Mobility.

PDF of AODV and DSR is higher than DSDV, TORA, ZRP protocols, as the speed of nodes increases PDR (Packet delivery ratio) of AODV and DSR increasing. PDR of DSDV is better at low mobility and worse under high mobility. ZRP perform better under low mobility but as the mobility increases PDR decreases. PDR of AODV lower than DSR due to higher rates of packets drop during discovery of routes. PDR Of TORA slightly less than DSR and AODV.DSR has the highest PDR.

5.3 ETE Delay in low movability of nodes and in low congestion

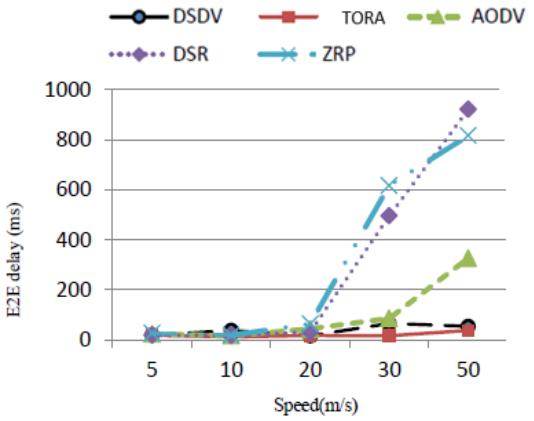


Fig. 3 ETE Delay Vs. Mobility.

For AODV E2E delay increases as speed nodes increases, due to high PDR packets reach at destination with minimum delay.E2E delay of DSDV is approximately same to AODV due to its unicast table-driven approach in case of node speed increases.E2E delay of DSR and TORA increases when speed of nodes increases due to its multihop routing. ZRP has the highest E2E delay with higher packet drop rates.

5.4 NRL in low movability of nodes and in low congestion

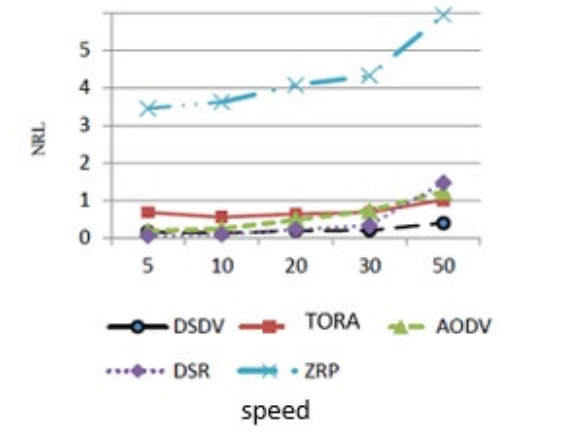


Fig. 4 NRL Vs. Mobility.

DSDV has least routing load under the network having low movability and low traffic, as the speed changes NRL remains consistent for DSDV.DSR has average routing load as the speed of nodes increases, as latest routes can be discovered from route cache. DSR works better for the network requires low movability and less traffic. NRL of AODV increases as node's speed increases because of more routes need to be discovered at route discovery phase as a result packet loss ratio increases. ZRP has highest NRL under low movability and less traffic networks.

6. Impact of high movability, or changing number of nodes.

In this paper proposed how performance parameters affect the network in terms of changing number of nodes and high mobility of nodes.

6.1 Evaluate throughput in high movability and in denser network

Initially throughput of all protocols is average for a network that contains only 30 to 40 nodes. But as the number of nodes increases throughput increases, Throughput of DSR decreases with increase number of nodes due to recent routes can be discovered from route cache. DSDV throughput increases due to high traffic and more flooding of control packets.

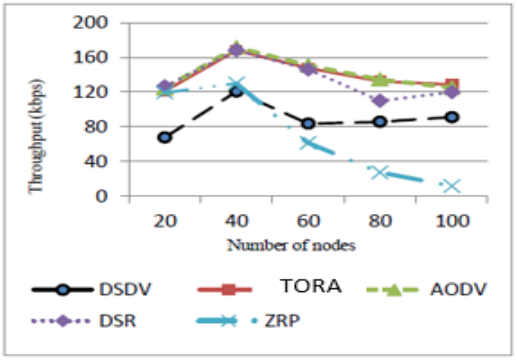


Fig. 1 Throughput V. No. of nodes.

6.2 Evaluate NRL in high movability and in denser network

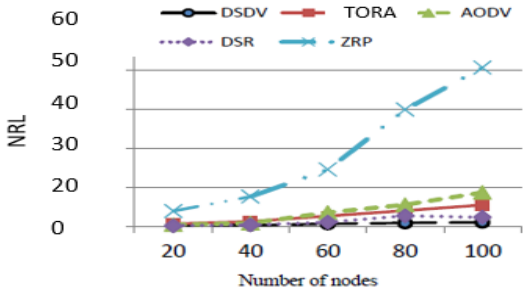


Fig. 2 NRL Vs. No. Nodes

NRL increasing as number of nodes increasing because more control packets interchanged with more neighbouring nodes. NRL of DSDV almost remains same as the number of nodes in the network increasing due to its flat routing scheme, performed well in dense network. NRL of DSR is greater than DSDV, as the network becomes denser more routes discovery involves, and route cache unable to discover its recent routes, hence packet loss ratio increases. NRL of TORA more than DSR in denser network. ZRP has the highest routing load among all protocols.

6.3 Evaluate PDF in high movability and in denser network

DSR ha highest PDF 99.76% among all protocols for network contains 30-40 nodes but as the nodes

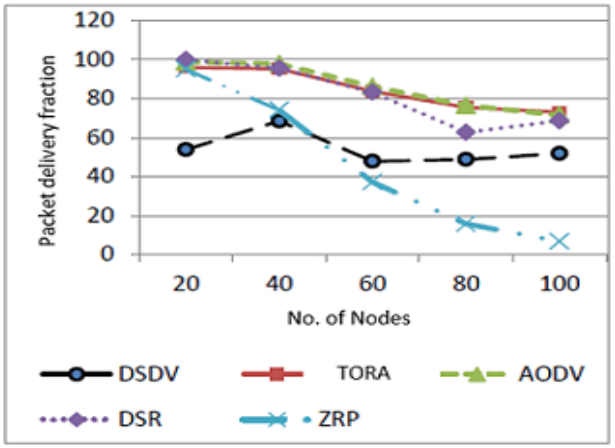


Fig. 3 PDF V. No. of Nodes

increases PDF of DSR decreases, AODV keeps stable PDF almost 86.7% in varying size networks. TORA sustains almost same packet delivery ratio 84.76% as AODV in term of network containing 100 nodes. PDF of ZRP is highest as 93.85% in network contains 40 nodes, but as nodes increases PDF decreases from 93% to 6% for the network contains 100 nodes.

6.4 Evaluate ETE Delay in high movability and in denser network

DSDV maintains constant delay time due to its proactive table-driven approach, DSDV less effected by the expanding number of nodes for network contains 20 to 100 nodes.E2E delay for DSR less but as the nodes increases network becomes congested, needs more time to packet delivery and routes discovery. AODV and TORA perform better in high traffic networks. ZRP delays changes as the number of nodes increases from 20 to 100 nodes. ZRP exhibits highest delay among all protocols.

Table 1: Comparison of protocols in terms of low movability and low traffic.

Parameters	ZRP	TORA	DSDV	DSR	AODV
PDF	0.780	0.850	0.860	0.983	0.910
NRL	0.050	0.030	0.001	0.004	0.003
ETE DELAY	680.4	8.74	8.34	674.56	38.94
THROUGHPUT	258.7	231.18	236.7	245.5	250.73

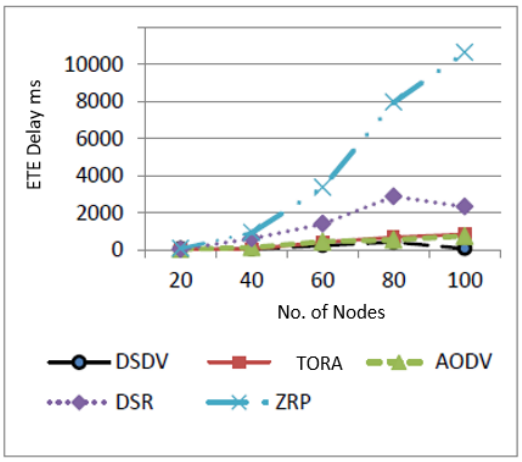


Fig. 4 ETE Delay V. No. of Nodes

Table 2: table Comparison of protocols in terms of high nodes' mobility and dense networks

Parameters	AODV	DSDV	DSR	TORA	ZRP
Throughput	148.67	339.27	146.71	233.7	127.2
ETE Delay	2705	2502	2788	3794	3996
PDF	0.0540	0.472	0.0360	0.0846	0.321
NRL	0.026	0.004	0.024	0.054	0.065

7. SECURITY issues in manet:

Ad hoc networking is easily targeted than wired networks. Because nodes are mobiles, they move freely in

the networks. Different factors influence the protection problems and architecture differently. Variables which affect the network security are: the dynamic environment, domain, Quality of service and critical state of security. Attacks[20] in ad hoc network can be classified in to two categories as Active and passive attacks. In active attacks the attacker tries to changes the communicated data or wants to disturb the network and when an attacker captures the data but does not disturb the network it is called passive attack. Many attacks faced in different layers but only network layer attacks (blackhole, wormhole and Gray hole attacks) will be discuss in this paper.

7.1 Blackhole attack and its detection:

Blackhole[20] is an active and routing layer attack using the reactive routing protocol.it is usually occur in the on-demand routing protocols for example AODV routing protocol which is discussed above in this section of review we precisely examine how Black Hole attack disturb the communication in AODV. In this attack attacker node shows the shortest route towards the destination and drops the packet that passes through this route instead of forwarding it and send the fake reply to source node. And whenever this route will be used to forward the packets malicious node will discard the packets.

For detection of blackhole attacks SAR[21] is used. Security aware ad-hoc routing protocol is used to prevent from this attack it uses concept of symmetric cryptography to encrypt and decrypt the packet. Every node in the network will have a shared secret for encryption and decryption. These keys will only be used by the authorized nodes so that they can encrypt and decrypt the packets and the malicious node cannot read the RREQ and RREP packets. In Security aware ad-hoc routing (SAR) a security metric is combined into the route request (RREQ) packet and route discovery process is followed. When middle nodes will receive the RREQ packet, they will check if it is secured then packet is forwarded to other neighbours. Else the packet is dropped. In SAR authentication and authorization are necessary to prevent from fraud.

7.2 Wormhole attacks and its detection:

Wormhole attacks[22] are also active attack because it captures the data and disturb the network performance they are often referred to as tunnelling attacks in which the intruder or malicious node collect packet in one area of the network and tunnels them to another place inside or outside the network, replaying the packets there. And the tunnel between these intruders is known as wormhole. It usually occurs in the DSR[23] protocol. In this protocol source routing is used to forward the packets from one node to another. DSR takes two steps which are Route Discovery and Route maintenance. Route discovery is used when the sender does not know about the route to their destination, then the sender will send the RREQ to other nodes. When a node will receive the RREQ it will check the id if it is the destination then it will send the RREP otherwise it will forward the packet to the other nodes. and. In route discovery when a route is found the no of hops, delays and time is kept in the routing table. For example, if route 1 is used for transmitting the packets and its hop count is decreased, we say that wormhole exist in this route. As in wormhole attack malicious node shows the shortest path and when the hop count is decreased wormhole can be identified. To detect this wormhole an encrypted message is send. Entire nodes in network add its key which is predefined in the network and only the valid nodes have the key. If all the nodes have added their key, we can say that it is normal route but if any node do not add their key the node is said to be wormhole. And the founded node is blacklisted so that this route will not be used for future communication. Wormhole can be easily detected by hop count but they can be prevented by only eliminating them from the network and destroy their path from the routing table.

7.3 Gray hole attack and its detection:

Another attack is “Gray hole attack” which is expansion [24]of blackhole. It is also an active attack and has two[25] phases. In the first step, a malicious node violates the AODV routing protocol to announce itself that it has a valid path to a destination for the purpose of diverting all the packets to the malicious route instead of genuine route and in the second step the malicious node drops the transferred packets with certain probability. Attacker node changes the behaviors rapidly. Thus, sometime it transfers packet and some time it drops the packets. Due to its dynamic nature it is very hard to find out such kind of attack in the network. DSR is used to detect the Gray Hole attack. Dynamic Source Routing statement is that all nodes will collaborate and without node collaboration in ad-hoc network, no route can be recognized and no packet can be forwarded. One method for the identification of Gray hole in AODV needs all nodes to preserve updated knowledge about their neighbours. After a period, tests every neighbour with whom it has not recently interacted, and begins the identification procedure for that node. When this node is found to be unsecure then it tells other suspect node’s neighbours to test it out and then then it takes a statement on the suspicious node.

Table 3: Comparison of network layer attacks' detection mechanism:

Detection Technique	simulator	Name of attacks	Source	Packet dropout rate	Transmission delay	Routing overhead
DPS (Detection prevention system) nodes[26]	NS-2	Black hole	addition of detective nodes	Reduce 13%-47% packet dropout rate in case of one black hole node and 28 %–45 % in case of two blackhole nodes	No transmission delays	No routing overhead Except sending threat message to other nodes
EMAODV[27]	NS-2	Black hole	Addition of control packets (SRRD-REQ and SRRD-REP) and threshold value	Packet delivery ratio is about 85% high than AODV	It requires more delay with respect to malicious node ratio	increase routing overhead compared to the AODV
Digital signature[28]	-	Worm hole	RREP/RREQ public key	Not defined	Comparable with AODV	Not defined
AODV[23]	NS-2	Worm hole	Smart packets and processing request	Only smart packets will be dropped by authorized nodes to ensure safe path	Not defined	Reduce routing overhead
Dynamic clustering technique[29]	-	Gray hole	AODV protocol with acknowledgement and MD5 algorithm for security	Packet delivery ratio is 0.44%	Transmission delay is o.167 seconds which is high when no of malicious nodes are high	11% routing overhead which is better than other technique like EAACK
SAODV[30]	NS-2	Gray hole	Opinion table and neighbour list	In comparison to the AODV Improvement in packet delivery ratio from 98.6%to 99.7%	Delay is minimum than AODV from 0.015 s to 0.010	Overhead is decreased to 9.42%

8. Conclusion:

In this paper a comprehensive literature reviewed on the topic of MANET. A detailed analysis of routing protocols and their classification, comparison of routing protocols under different network scenarios, security attacks, detection of these attacks have been studied. In this paper we reviewed the comparison of AODV, DSDV, TORA, DSR and ZRP on evaluation metrics under two network scenarios low movability of nodes in low denser network and high movability of nodes and high denser network.

From table 4 given below, we concluded that Reactive protocols performed well over Proactive in respect of PDR and Throughput and Proactive protocols perform better than Reactive in regard with ETE delay and NRL in both scenarios. The overall performance of AODV, DSR better than TORA, ZRP.ZRP showed poorest performance in all scenarios while DSDV exhibits average performance

Table 4: Rank wise evaluation of routing protocols in relation to node's mobility

Parameters	ZRP	TORA	DSDV	DSR	AODV
ETE Delay	Highest	Lower	Lowest	Higher	High
Throughput	Lowest	High	Average	Higher	Highest
PDF	Low	High	Lowest	Highest	Higher
NRL	Highest	High	Lowest	Lower	Low

From table 5 given below, Performance of TORA is good under high movability and in high traffic networks in regard with PDR, but NRL of TOR is high in both networks. Throughput of TORA is high in dense networks. DSDV performed better in regard with least normalized routing load and ETE delay.

Table 5: Rank wise evaluation of protocols in relation to dense network

Parameters	ZRP	TORA	DSDV	DSR	AODV
ETE delay	Highest	High	lowest	low	Average
PDF	lowest	High	low	Average	Highest
NRL	Highest	High	Lowest	low	Average
Throughput	lowest	low	High	Average	Highest

Further we have discussed network layer attacks Black Hole, Worm Hole and Gray Hole and their detection mechanism. Moreover, we have analysed comparison of different techniques which are used to prevent these attacks. This comparison was in tabular form and based on three performance metrics i.e. packet dropout rate, transmission delay and routing overhead. It is concluded that many techniques give us protection /detection against these attacks but transmission delay in some techniques is increased and minimized but is not fully handled. Therefore, it is need for detection/prevention technique which can fully recover it

REFERENCES:

[1] G. Jayakumar and G. Gopinath, "Ad Hoc Wireless Networks Routing Protocols - A Review," Journal of Computer Science, vol. 3, no. 8. pp. 574–582, 2007.

[2] A. Hinds, M. Ngulube, S. Zhu, and H. Al-Aqrabi, "A Review of Routing Protocols for Mobile Ad-Hoc NETworks (MANET)," Int. J. Inf. Educ. Technol., vol. 3, no. 1, pp. 1–5, 2013.

[3] A. Gupta, "Review of Various Routing Protocols for MANETs," Int. J. Inf. Electron. Eng., vol. 1, no. 3, 2011.

[4] S. Prakash, R. Kumar, B. Nayak, and M. K. Yadav, "A Survey on Reactive Protocols for Mobile Ad Hoc Networks (MANET)," Proc. 5th Natl. Conf. INDIACom-2011, 2011.

[5] S. Kumar, M. Goyal, D. Goyal, and R. C. Poonia, "Routing protocols and security issues in MANET," 2017 Int. Conf. Infocom Technol. Unmanned Syst. Trends Futur. Dir. ICTUS 2017, vol. 2018-Janua, no. 4, pp. 818–824, 2018

[6] A. Bhattacharyya, A. Banerjee, D. Bose, H. N. Saha, and D. Bhattacharjee, "Different types of attacks in Mobile ADHOC Network: prevention and mitigation techniques," Dep. Comput. Sci. Eng. Inst. Eng. Manag. Saltlake, vol. 1, no. 1, 2011.

[7] P. Manickam and T. G. Baskar, "P ERFORMANCE C OMPARISONS OF R OUTING P ROTOCOLS IN M OBILE A D H OC N ETWORKS," vol. 3, no. 1, pp. 98–106, 2011.

[8] M. K. Gulati and K. Kumar, "Performance Comparison of Mobile Ad Hoc Network Routing Protocols," Int. J. Comput. Networks Commun., vol. 6, no. 2, pp. 127–142, 2014.

[9] H. Narra, Y. Cheng, E. Çetinkaya, J. Rohrer, and J. Sterbenz, "Destination-Sequenced Distance Vector (DSDV) Routing Protocol Implementation in ns-3," no. March, 2012.

[10] K. E. Kannammal and T. Purusothaman, "An efficient routing protocol for wireless sensor networks," Life Sci. J., vol. 10, no. 2, pp. 1650–1653, 2013.

[11] C. Cheng, R. Riley, S. P. R. Kumar, and J. J. Garcia-Luna-Aceves, "Loop-free extended Bellman-Ford routing protocol without bouncing effect," pp. 224–236, 1989.

[12] X. Hong, K. Xu, and M. Gerla, "Scalable routing protocols for mobile ad hoc networks," IEEE Netw., vol. 16, no. 4, pp. 11–21, 2002.

[13] R. V Boppana and A. Mathur, "Analysis of the Dynamic Source Routing Protocol for Ad Hoc Networks," Computer (Long. Beach. Calif)., no. December, pp. 1–8, 2005.

[14] N. Beijar, "Zone Routing Protocol (ZRP)," Netw. Lab. Helsinki Univ. Technol. Finl., pp. 1–12, 2002.

[15] S. Barakovi, S. Kasapovi, and J. Barakovi, "Comparison of MANET Routing Protocols in Different Traffic and Mobility Models," Telfor J., vol. 2, no. 1, pp. 8–12, 2010.

[16] S. Gandhi, N. Chaubey, N. Tada, and S. Trivedi, "Scenario-based performance comparison of reactive, proactive & hybrid protocols in MANET," 2012 Int. Conf. Comput. Commun. Informatics, ICCCI 2012, pp. 0–4, 2012.

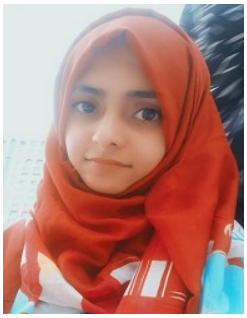
[17] A. U. Salleh, Z. Ishak, N. M. Din, and M. Z. Jamaludin, "Trace analyzer for NS-2," SCOReD 2006 - Proc. 2006 4th Student Conf. Res. Dev. "Towards Enhancing Res. Excell. Reg., no. SCOReD, pp. 29–32, 2006.

[18] K. Rampurkar, N. Lavande, S. Shilgire, and S. N. Mane, "Study of Routing Overhead and its Protocols," Int. J. Adv. Eng. Manag., vol. 2, no. 2, p. 52, 2017.

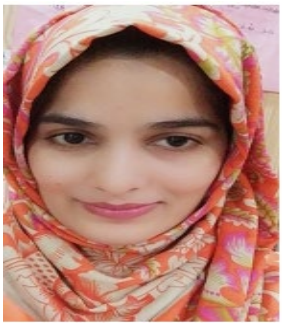
[19] D. Kaur and N. Kumar, "Comparative Analysis of AODV, OLSR, TORA, DSR and DSDV Routing Protocols in Mobile Ad-Hoc Networks," Int. J. Comput. Netw. Inf. Secur., vol. 5, no. 3, pp. 39–46, 2012.

[20] S. N. Mohammad, "Security Attacks in MANETS (Survey Prospective)," Int. J. Eng. Adv. Technol., no. 3, pp. 2249–8958, 2017.

[21] T. P. Venkatesan, "Security Attacks and Detection Techniques for MANET," no. April 2014, 2017.
[22] P. Panda, K. K. Gadnayak, and N. Panda, "SURVEY ARTICLE MANET Attacks and their Countermeasures : A Survey," vol. 2, pp. 319–330, 2013.
[23] A. Aashima and V. K. Arora, "Detection and Prevention of Wormhole Attack in MANET Using DSR Protocol," IOSR J. Comput. Eng., vol. 16, no. 6, pp. 44–47, 2014.
[24] R. Sharma, "Gray-hole Attack in Mobile Ad-hoc Networks : A Survey," vol. 7, no. 3, pp. 1457–1460, 2016.
[25] J. Sen, M. G. Chandra, S. G. Harihara, H. Reddy, and P. Balamuralidhar, "A Mechanism for Detection of Gray Hole Attack in Mobile Ad Hoc Networks," pp. 0–4, 2007.
[26] M. G. Pineda, J. Lloret, S. Papavassiliou, S. Ruehrup, and C. B. Westphall, "Ad-hoc networks and wireless: ADHOC-NOW 2014 International workshops ETSD, MARSS, MWaoN, SecAN, SSPA, and WiSARN Benidorm, Spain, June 22-27, 2014 revised selected papers," Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics), vol. 8629, no. June, pp. 5–6, 2015.
[27] A. Rana, V. Rana, and S. Gupta, "EMAODV : TECHNIQUE TO PREVENT COLLABORATIVE ATTACKS IN MANETs," vol. 70, pp. 137–145, 2015.
[28] N. Gupta and S. N. Singh, "WORMHOLE," pp. 3–6, 2016.
[29] S. U. Patil, "Gray hole attack detection in MANETs," 2017 2nd Int. Conf. Converg. Technol. I2CT 2017, vol. 2017-Janua, pp. 20–26, 2017.
[30] S. Dhende, S. Musale, S. Shirbahadurkar, and A. Najan, "SAODV: Black hole and gray hole attack detection protocol in MANETs," Proc. 2017 Int. Conf. Wirel. Commun. Signal Process. Networking, WiSPNET 2017, vol. 2018-Janua, no. March, pp. 2391–2394, 2018.



Amina Yaqoob received BS(IT) degree from University of Gujrat in 2017, working as SSE(CS) in Punjab Education Department, and now doing Masters in department of Computer Science and Information Technology in University of Lahore Pakistan, Gujrat campus. Current research areas and interests are networks, machine learning.



Alma Shamas received degree of BS(IT) from University of Gujrat Hafiz Hayat Campus in 2017, after that working as SSE(CS) in Punjab Education Department in Sialkot. Further doing masters in Department of Computer Science and Information technology in University of Lahore Pakistan, Gujrat Campus. Current research areas and interests are networks, machine learning.

Dr. Muhammad Sultan Zia received degree in Masters of Sciences in Software Engineering, working as an Associate Professor, Head of Department at Department of Computer Science and Information technology in University of Lahore, Campus Gujrat.