INTERNATIONAL JOURNAL FOR ADVANCE RESEARCH IN ENGINEERING AND TECHNOLOGY

WINGS TO YOUR THOUGHTS…..

HIT AND MISS: A HAPHAZARD ZONE PANEL PROTOCOL FOR MANETs

S.Neelavathy pari[1], D.Kalpana[2], D.Sridharan[3], P.Sathyaraj[4]

[1]Assistant Professor, Department of Computer Technology, MIT Campus, Anna University.
[2]Assistant Professor, Department of CSE, RMD Engineering College, Anna University.
[3]Associate Professor, Department of ECE, CEG Campus, Anna University.
[4]Assistant Professor, Department of ECE, RMK College of Engineering and Technology, Chennai.
shakthi.kalpu@gmail.com

***Abstract**—In this paper, we address the problem of providing anonymity protection in Mobile adhoc networks (MANETs) using a haphazard zone panel protocol (HZP). The HZP protocol offers anonymity protection to sources, destinations, and routes. It uses the partitioning technique and chooses the random forwarder (RF) to forward the packets to the destination. In HZP protocol the Random forwarder (RF) node is selected based on the fidelity level of the neighbor nodes. So HZP protocol uses shortest path and routes the packets. Hence the packet drop, delay is reduced and throughput gets increased. The malicious node gets eliminated based on fidelity factor. GPSR (Greedy Perimeter Stateless Routing) forwards the packets to the node which is closest to the destination node by periodically broadcasting the beacon packets to every node in the zone. The simulation result shows that HZP protocol has improved the packet delivery ratio, throughput and delay, compared with ALERT protocol.*

***Index Terms**- Mobile adhoc network, Random forwarder, Greedy Perimeter Stateless Routing, Fidelity level.*

1. INTRODUCTION

Mobile Ad hoc Network (MANET) is a group of wireless mobile hosts, which has no stationary infrastructure or base station for communication. The nodes act as routers for forwarding and receiving packets to/from other nodes. Ad hoc networking are extensively use for military purposes, disaster relief, mine site operation, etc. For such applications, a secure and reliable communication is necessary. Routing in ad hoc networks has been a challenging task ever since wireless networks came into existence. Therefore a dynamic routing protocol is needed for the MANET networks to function properly.

Anonymous routing protocols are important in MANETs to provide secure communications by hiding node uniqueness and preventing traffic analysis attacks from outside observers. “Uniqueness of a node and location anonymity of sources and destinations” means it is hard to find the node distinctiveness and exact locations of the sources and destinations [1]. There are many anonymous routing protocol available ALARM (Anonymous Location Aided Routing in suspicious MANETs), AO2P (Ad hoc On-Demand Position-Based Private Routing Protocol),GPSR [6][10].ALERT provides location anonymity by hiding node identities using dynamic fictitious name [1].It hides the MAC address and the pseudonym will be changed often at particular time gap. Packets are forwarded by choosing random nodes by partitioning the network into two zones. The random forwarder is chosen by geographic routing protocol (GPSR)[2][6]. GPSR selects the nodes which are very closer to the destination. Since each time random nodes are selected to forward the packets it is hard to trace the path by the attacker. As the number of random forwarder increases the packets are more secured but the delay gets increased. Haphazard Zone Panel Protocol Partitions the given MANET network into vertical zones and chooses random forwarder by GPSR. With the growing popularity of positioning devices (GPS)[6], the geographic routing protocols (GPSR) are becoming an attractive choice for use in MANET. The GPSR needs to know the final destination and position of neighbor nodes. The sender and destination node is stored in location service (ie, Grid Location System GLS)[2][5].The location service is duplicated to all the nodes in network. Since the nodes in MANET are mobile nodes, each node broadcasts its updated location information to its neighbors. These updated packets are called beacons. It forwards the beacon packets periodically to the neighbor nodes. This packet is also broadcasted to nodes which are at rest. So it keeps the location of the neighbor’s node up to date. The source and destination ID is not exposed to neighbor node. It uses false name called dynamic fictitious name to hide MAC address. The fictitious name changes frequently to avoid tracing the routing path.

The rest of the paper is organized as follows: section II presents a literature review, Section III description of the proposed work. Detail description about Implementation of HZP protocol with simulation analysis is presented in section III. Finally section IV concludes the work and the future enhancement.

2. LITERATURE REVIEW

While packet forwarding to different routes the forwarding protocol provides better protection for maintaining privacy, high quality of services both success ratio and delay, and also reduces the overhead. The malicious activity might be due to selfishness (to save battery power), intentional or because of the faulty or broken links.

Quanjun Chen [1] proposed that periodic distribution of beacon packets that contain the geographic location coordinates of the nodes is a widely held method used by most geographic routing protocols to maintain neighbor locations. Periodic beaconing regardless of the node flexibility and traffic patterns in the network is not attractive from both update cost and routing performance points of view. Adaptive Position Update (APU) plan for geographic routing, which dynamically changes the frequency of position updates based on the movement of the nodes and the forwarding patterns in the network. APU is based on two simple ethics:

- Nodes whose movements are tougher to calculate update their positions more often (and vice versa), and
- Nodes nearer to forwarding routes update their positions more often (and vice versa).

APU can significantly decrease the location update cost and increase the packet routing performance in terms of packet delivery ratio and average end-to-end delay. It is essential that every node broadcasts its updated location information to all of its neighbors. These location update packets are usually referred to as beacons. APU includes two rules for activating the beacon update process. The first rule, discussed as Mobility Prediction (MP), uses a simple mobility prediction pattern to estimate when the position information broadcast in the former beacon becomes incorrect. The second rule, discussed as On-Demand Learning (ODL), aims at improving the exactness of the topology along the routing routes between the communicating nodes [1]. ODL uses an on-demand learning plan, whereby a node broadcasts beacons when it overhears the transmission of a data packet from a new neighbor in its locality.

Author [3] proposed that protocols for secure routing are either proactive or reactive in approach. The proposed protocol is based on the idea zone routing protocol (ZRP) which employs an integrated approach of digital signature and both the symmetric and asymmetric key encryption methods to attain the security goals like message integrity, data privacy and end to end authentication at IP layer.

The reasons for choosing ZRP as the source of our protocol are as follows:

(i) ZRP is based on the idea of routing zones, a limited area, and it is more possible to apply the security mechanisms within a limited area than in a wider area that of the entire network,

(ii) Since the idea of zones separate the communicating nodes in terms of internal and external nodes, certain information like network topology and neighborhood information etc. can be hidden to the external nodes,

(iii) In case of a failure, it can be limited to a zone. As the data packets are usually long and symmetric key approach is faster than the asymmetric key encryption. We encrypt all the data packets using the symmetric key approach. Each communicating node has two pairs of private/public keys, one for signing and verifying and the other for encrypting and decrypting. The secure intra zone routing protocol (SIARP) is a limited depth proactive link-state routing protocol with inbuilt security features. It periodically calculates the path to all intra zone nodes and sustains this information in a data structure called SIARP routing table. This process is called proactive route computation. SIERP is a reactive routing protocol with extra security features. It offers on demand secure route discovery and route maintenance services based on local connectivity information monitored by SIARP. NDP does this by periodically transmitting a HELLO beckon to the neighbors at each node and updating the neighbor table on receiving similar HELLO beckons from the neighbors. NDP gives the information about the neighbors to SIARP and also alerts SIARP when the neighbor table updates.

K.E. Defrawy [2] proposed when comparing with most networks, where communication is based on long-term addresses, we claim that the location-centric communication paradigm is better-suited for privacy in suspicious MANETs. To this end, we construct an on-demand location-based anonymous MANET routing protocol (PRISM) that attains privacy and security against both outsider and insider adversaries. A passive outsider overhears on all communication and aims to compromise privacy, i.e., track nodes. An active outsider can inject, change and replay messages in addition to chasing nodes. A passive insider obtains messages exchanged within the MANET and externally behaves correctly by following all rules and protocols. Active insiders are the most powerful adversary type. The basic process of PRISM is like AODV. PRISM allows a source to specify a destination area and concurrently discover multiple destination nodes in it.

Sanjay K. Dhurandher [6] proposed a new principle which offers secured routing by means of a protocol named FACES. This algorithm works by sending challenges and distribution friend Lists to offer a list of confidential nodes to the source node through which data transmission finally takes place**.** As a result of this operation, the network is able to efficiently segregate the malicious nodes in the ad hoc network. The information about the malicious nodes is collected successfully by using Challenges. This decreases the overhead on the network significantly. Through extensive simulation analysis it was inferred that this pattern provides an efficient approach towards security and easier detection of malicious nodes in the mobile ad hoc network.

Karim El Defrawy [9] proposed by speaking number of problems arising in suspicious location-based MANET by designing and examining a privacy-preserving and protected link-state based routing protocol (ALARM). ALARM uses nodes’ current positions to securely disseminate and build topology snapshots and forward data. With the help of advanced cryptographic methods (e.g., group signatures), ALARM offers both security and privacy features, as well as node authentication, data integrity, anonymity, and tracking-resistance. It also offers protection against passive and active insider and outsider attacks. To the best of our knowledge, this work signifies the first comprehensive study of security, confidentiality, and performance tradeoffs in the context of link-state MANET routing.

X. Wu [5] proposed Mobile Ad hoc network (MANET) is one of the most important and unique applications. On the contrary to outdated network architecture, MANET does not need a static network infrastructure; every single node works as both a transmitter and a receiver. Nodes communicate directly with each other when they are both inside the same communication range. Else, they rely on their neighbors to send messages. The self-configuring ability of nodes in MANET made it popular among dangerous mission applications like military use or emergency retrieval. However, the open medium and wide scattering of nodes make MANET vulnerable to malicious attackers. In this case, it is critical to improve efficient intrusion-detection mechanisms to protect MANET from attacks. With the enhancements of the technology and cut in hardware costs, we are observing a recent trend of expanding MANETs into industrial applications. To adjust to such trend, we strongly trust that it is vital to address its potential security problems.

Elhadi M. Shakshuki [10] proposed anomaly based intrusion detection system used for detecting computer intrusions and exploitation by monitoring system activity &categorizing it based on rules such as signatures or patterns.

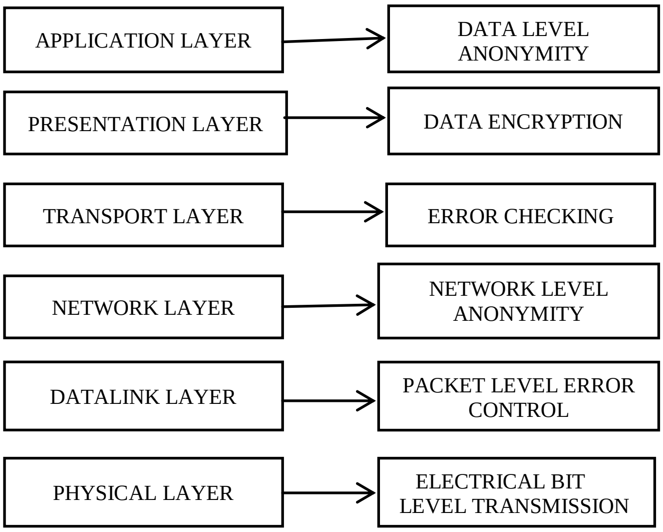

Figure 1: Anonymity in MANETs

Anonymity protection in MANETs is established by preserving confidentiality of user data. The figure 1 depicts the anonymity in MANETs. The user data in the application layer is data level anonymity. Hiding network identifiers of communication partners in network layer is the network level anonymity.

3. PROPOSED SYSTEM

Haphazard Zone Panel Protocol hides node id, position of source and destination, and packet forwarding route. It chooses the neighbor node based on the fidelity value. To make it clear in unique sentence, “fidelity is a counter that is associated with a node, which is increased each time it forwards a packet successfully”. Each and every time when a node arrives into a network its fidelity is one and every time when it goes permanently off from the network its value is again restored to one. When a node forwards any data packet successfully it will always increase a counter value and that is the fidelity value of that particular node. Source node selects the node which has maximum fidelity value to forwards data packets. So the packet delivery ratio and throughput is increased by detecting the malicious node in the zone. The behavior of malicious node will drop or misroute the packets. The malicious node can be identified by route request (RREQ) and route response(RREP).The initiator node sends the RREQ message to its neighbor nodes. Neighbor nodes sends RREP to sender and the first reply will be omitted.

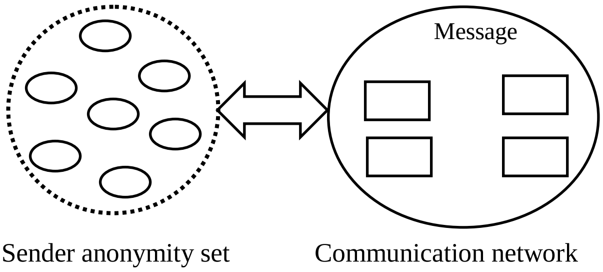

Figure 2: Sender Anonymity

The zones partitions are done in haphazard zone panel protocol are as follows: Each data initiator or forwarder executes the hierarchical zone partition. The partition is first done vertically. The area is first divided into two zones as A and B. We then horizontally partition zone B as B1and B2. After that we vertically partition zone B1as B11 and B12.Such partition divides into smallest zone into alternative vertical and horizontal manner. In HZP protocol partitioning is done for a particular time stamp.

Figure3 illustrates the method of dividing zones by using HZP. The routing in HZP, where S is source zone and D is destination zone and is denoted as Z_{D}. Specifically, in the HZP routing, each data source or forwarder executes the zone partition. It first finds whether it and destination are in the same sector. It alternatively divides the zones in horizontal and vertical directions. The node repeats the same process itself until Z_D are not in the same zone. Then it randomly chooses a position in other zone called temporary zone (TD). It uses a GPSR routing algorithm to send the node closest to TD. This node is defined as Random forwarder (RF).

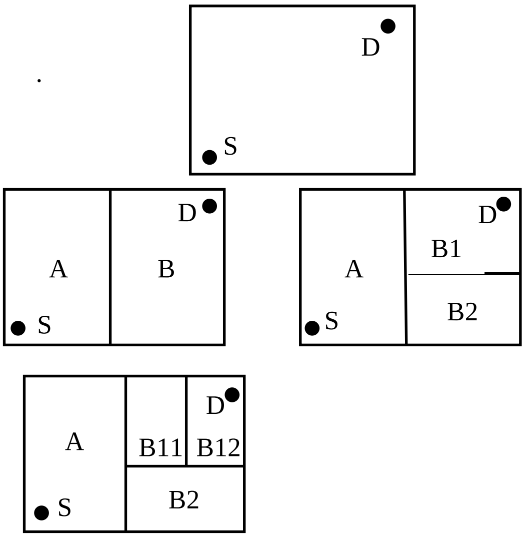

Figure 3: Zone partition in HZP.

3.1 GPSR ROUTING ALGORITHM:

Greedy Perimeter Stateless Routing, GPSR is a reactive and efficient routing protocol for mobile ad hoc networks. In contrast to routing algorithms implemented before, using the concepts of graph theory, the shortest path and transitive accessibility to find routes, GPSR exploits the correspondence between the position and connectivity in a wireless network, using the positions of the nodes to make packet forwarding decisions. Let (X_D, Y_D) and $(X_{F,}\ Y_F)$ respectively denotes the locations of the destination node D and the Forwarding node F that has the data packets to be forwarded to D. The below GPSR algorithm illustrates the code for GPSR protocol. The F node calculates the distance between itself and the destination node D and also distance between each of its neighbor node N_K and D. If a neighboring node N_K of the random forwarding node RF is relatively closer to D, then the progress(ie, fraction of the distance covered) with the potential selection of N_K as the next hop node would be the difference in the distance between N_K and D divided by the destination between F and D. Among such neighbor noes, the node that has the maximum value for the progress is the node that lies closest to the destination and is chosen by F as the next hop to forward the data packet. If the F couldn't find a neighbor node that lies closer to the destination than itself, then the node switches to perimeter mode.

```
Algorithm for GPSR Packet Forwarding.
Input:Forwarding Node F, Destination D, Neighbor-List (L)
Output: Next-Hop-Node   // if greedy forwarding successful
   NULL                 // if not successful
Initialization: Next-Hop-Node=NULL
        Maximum progress=0
Begin                   //GPSR greedy Forwarding

Distance $_{RF-D}$= $\surd\,(X_F – X_D)^2 + (Y_F – Y_D)^2$
For every neighboring node $N_K$ € Neighbor-List (L) do
 Distance $_{K-D}$ = $\surd\,(X_K – X_D)^2 + (Y_K – Y_D)^2$
 If (Distance $_{K-D}$ < Distance $_{F-D}$) then
Progress (F, K) = (Distance $_{F-D}$ - Distance $_{K-D}$) / (Distance $_{F-D}$)
If (Maximum-progress <Progress (F, I)) then
        Maximum-progress =Progress (F, I)
        Next-Hop-Node = 1
    End if
   End if
End for
If (Maximum-Progress > 0) then
    Return Next-Hop-Node//greedy forwarding
    Else return NULL // greedy forwarding failure
 End if
End GPSR greedy forwarding algorithm
```

Features of the proposed Hit and miss: Haphazard zone panel protocol is as follows:

i)**Low cost**: Lower cost among all the existing protocols such as ALARM, ZAP, SDDR, and ALERT.

ii).**Dynamic partition:** Partioning is done dynamically to reduce network overhead.

iii)**Anonymity protection:** Provides Anonymity protection even to non-traceable path.

iv) **Strategy to strengthen privacy:**Hides data initiators among more number of initiators.

v)**k-anonymity protection**: HZP Provides k-nodes in the destination by using k-anonymity.

vi) **Pliable to Intersection and timing attacks:** HZP is very flexible to the attacks in MANETs.

3.2 HZP ROUTING PROTOCOL:

The algorithm for the HZP protocol is written and implemented using network simulator. In HZP protocol the network zone is vertically split it into two zones A and B, if the Source and destination are in same zone. A temporary destination TD1 is selected in zone A using GPSR algorithm. This TD1 selects random forwarder (RF1) in zone B. this process is continued till source and destination are not in same zone. A time stamp is ONed and partitioning is done till the time expires. Then the source broadcasts the RREQ to all nodes and collects RREP. Source selects the node with highest fidelity level and sends the data to the destination, if the data successfully forwarded then the fidelity value is increased otherwise the fidelity value will de decremented. If any malicious node is present the value will be zero, and alarm message will be sent to the other nodes. The below algorithm illustrates the code for HZP routing protocol. Initially the network zone is considered to be rectangle and nodes are distributed randomly. Here the implementation is done for forty nodes and a source and destination node is chosen and hierarchical partitioning is done for a particular time stamp (Ti) until S and D are not in same zone. Source broadcast RREQ to nodes and collects RREP and maintains in a routing table till Ti expires. If routing table entry is zero nodes S retransmits RREQ packets and collects the reply. Based on that fidelity value a neighbor node is chosen and if any node having its value zero then that node is removed from the table since it is a malicious node and sending alarm message to all the other nodes.

NND Pseudo code:

Nearest Neighbor Destination Algorithm is used for zone partitioning in HZP protocol.

Input: Source -S & Destination- D, T_i-time stamp

Output: Node waiting time -ACK_TIMEOUT

Assumption: Network area is rectangular & nodes are distributed randomly.

```
1:  Initialize (P);              //Partitioning is performed
2:  Intialize (V);              //Vertical partitioning
3:  Intialize (H);             //Horizontal partitioning
4: S←node 0 to 39 do
5:   D←node 1 to 39 do
6:  for $T_i$=1 to simclock do   //Checks for Timestamp $T_i$=1
7:  Partition the zone vertically [A,B]
8: Chooses nodes in zones as IR
9:  repeat step 7 until S&D are not in the same zone
10:  else randomly choose A1← TD1
11: S relies on GPSR to send packet S→TD1
12: then RF1 partitions A1 to B1 and B2
13:RF1 chooses next TD2
14: repeat step 13 until packet resides in destination zone
15: Partition until particular $T_i$
16: endfor Ti
```

```
S→BRREQ to neighbor's      //Broadcasts repeat request
if(simclock=current_time+RREP_max_time
return RT            //Routing Table
if size(RT) =0 retransmit RREQ
return R←HFL
otherwise LFL- - deleted
if FL=1
Remove node from RT
then broadcast alarm packets end
```

3.3 *SIMULATION ENVIRONMENT:*

The simulation of ALERT and HZP protocol was done in NS-2.33, using the wireless extensions. This simulation environment offers high fidelity, as it includes full simulation of the IEEE 802.11 physical and MAC layers.
The NS-2.33 wireless simulation model simulates nodes moving in an unobstructed plane. Motion follows the random way point model a node chooses a destination uniformly at random in the simulated region, chooses a velocity uniformly at random from a configurable range, and then moves to that destination at the chosen velocity. Upon arriving at the chosen waypoint, the node pauses for a configurable period before repeating the same process. In this model, the pause time acts as a proxy for the degree of mobility in a simulation; longer pause time amounts to more nodes being stationary for more of the simulation.

3.4 *SIMULATION PARAMETERS:*

We implement our proposed anonymous routing protocol on network simulator 2.33 using 802.11 as the MAC protocol. The matrices we mainly focused are packet delivery ratio, throughput, end to end delay. We setup scenario with a terrain size 1500mX700m and place 40 nodes in it. The packet size used is 2000bytes. The code for GPSR module is simulated and the various parameters are measured like throughput, packet delivery ratio. Table 1 shows the different configuration parameters send to setup the scenario.

Table 1: Simulation parameters

Terrain	1500mx700m
Antenna model	Omni Directional
Routing Protocol	AODV
Propagation	Two Ray ground
Simulation time	40s
Packet size	512bytes
Number of Nodes	40,60,80,100
Node mobility	10m/s,20m/s,30m/s

1. PACKET DELIVERY RATIO:

$$\text{Packet Delivery Ratio} = \frac{\sum \text{Total packets Received by all the Destination node}}{\sum(\text{ Total packets Sent by all the Source node})}$$

2. AVERAGE END TO END DELAY:

$$\text{Average End to End delay}(\mathrm{D}) = \frac{1}{\mathrm{n}\{\sum(\mathrm{Tri} - \mathrm{Tsi}) * 1000\}(\mathrm{ms})}$$

D=Average End to end delay
i=packet identifier
Tri=reception time
Tsi=Sender time
n=Number of packets successfully delivered

3. AVERAGE THROUGHPUT:

$$\text{Average throughput} = \frac{\text{Received size}}{\text{stop time} - \text{start time}} * \left(\frac{8}{1000}\right)$$

Received size=stored received packet size
Stop time=simulation stop time.

4. EXPERIMENTAL RESULTS

The following tables show the simulation results of HZP protocol. This shows that the HZP protocol performs better when compared to ALERT.

Table 2: Performance of ALERT and HZP with varying number of nodes and mobility speed is 10m/s.

Count of nodes with speed 10m/s	ALERT			HZP		
	Packet delivery ratio	Through put	Delay	Packet delivery ratio	Through put	Delay
40	0.9989	53.45	46.4	0.9996	58.47	31.35
60	0.9983	40.87	59.4	0.9991	46.35	35.28
80	0.9975	37.15	156.8	0.9988	42.58	114.2
100	0.9961	35.88	275	0.9975	39.72	219.2

Table 3: Performance of ALERT and HZP with varying number of nodes and mobility speed is 20m/s.

Count of nodes with speed 20m/s	ALERT			HZP		
	Packet delivery ratio	Through put	Delay	Packet delivery ratio	Through put	Delay
40	0.9983	45.34	133.4	0.9989	52.42	108.5
60	0.9969	39.71	211.4	0.9978	44.97	173.1
80	0.9955	35.00	289.4	0.9965	39.88	242.8
100	0.9946	31.96	323.5	0.9962	39.17	268.4

Table 4: Performance of ALERT and HZP with varying number of nodes and mobility speed is 30m/s.

Count of nodes with speed 30m/s	ALERT			HZP		
	Packet delivery ratio	Through put	Delay	Packet delivery ratio	Through put	Delay
40	0.9981	43.34	211.4	0.9990	48.93	175.4
60	0.9963	38.14	237.4	0.9981	39.62	181.8
80	0.9954	34.68	306.1	0.9978	37.12	245.6
100	0.9934	30.25	344.2	0.9968	37.74	267.8

Figure 5 illustrates number of nodes versus packet delivery ratio for varying number of nodes. HZP protocol performs better when compared to ALERT for various numbers of nodes and the mobility speed of the node is kept as 10m/s.

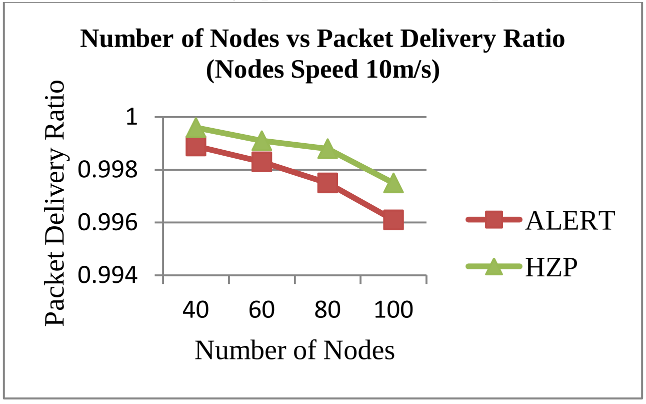

Figure 5: Number of Nodes vs Packet Delivery Ratio with mobility of node is 10m/s.

Figure 6 illustrates graph for Number of nodes versus packet delivery ratio with nodes mobility speed is changed to 20m/s.

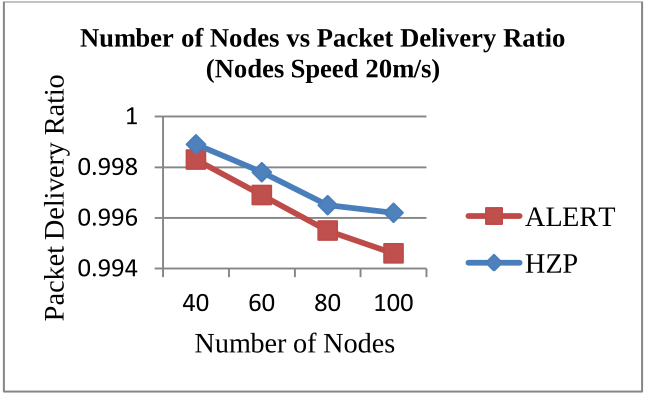

Figure 6: Number of Nodes vs Packet Delivery Ratio with mobility of the node is 20m/s.

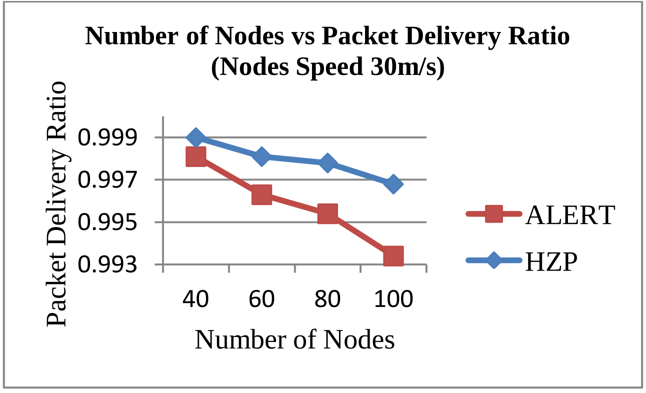

Figure 7: Number of Nodes vs Packet Delivery Ratio with mobility of node is 30m/s.

Figure 7 illustrates graph for Number of nodes versus packet delivery ratio. Packets are delivered by setting node speed as 30m/s and HZP protocol performs better when compared to ALERT.

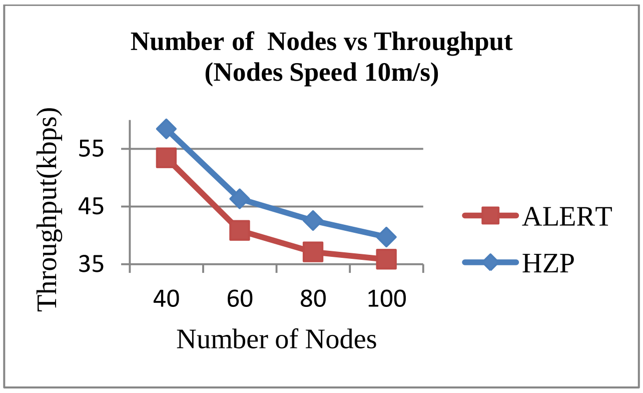

Figure 8: Number of Nodes vs Throughput with mobility of node is 10m/s.

Figure 8,9,10 illustrates that number of nodes versus throughput for varying number of nodes and speed of the node is changed to 10m/s, 20m/s, 30m/s. when compared to ALERT, HZP protocol performs well.

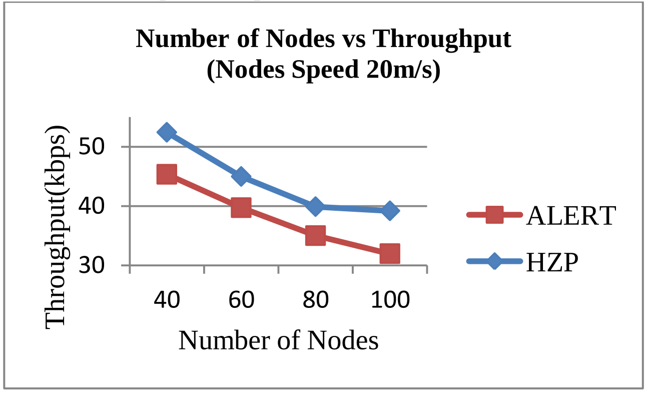

Figure 9: Number of Nodes vs Throughput with mobility of node is 20m/s.

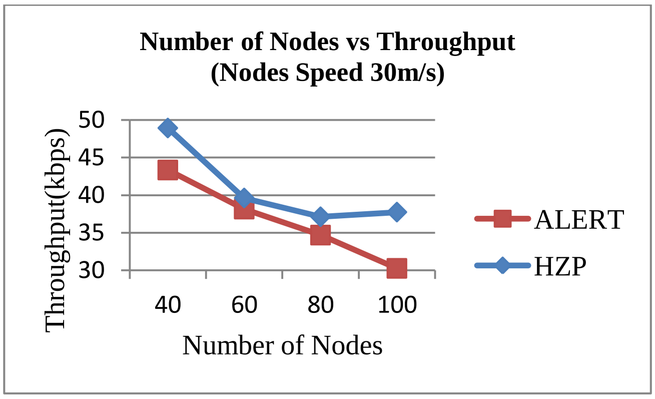

Figure 10: Number of Nodes vs Throughput with mobility of node is 30m/s.

5. CONCLUSION & FUTURE ENHANCEMENT

To improve packet delivery ratio and throughput we introduce new switching mechanism called Haphazard zone panel protocol for MANETs, which reduces network delay.
ALERT does not choose relay node with GPSR algorithm, instead it randomly chooses the relay nodes. It only uses GPSR for data transfer from relay node to relay node. The HZP protocol uses each node to maintain a neighbor list

with reliable level of its entire neighbor. Reliable level of each node is determined by its forwarding ratio. Now all the nodes have its neighbor node reliability level .If there is any malicious node in network the reliability level should be less. So the malicious node cannot be a forwarder node. This makes the update cost is increased in HZP protocol.

REFERENCES

[1] Quanjun Chen, Salil S. Kanhere&Mahbub Hassan, 'Adaptive position update for geographic routing in MANETs', IEEE transactions on mobile computing,vol.9,pp.4046-4051,2013.

[2] K.E. Defrawy& G. Tsudik, 'PRISM: Privacy-Frindly Routing in Suspecious MANETs and VANETs', proc. IEEE Int'l Conf.Network Protocols (ICNP),pp.258-267,2011.

[3] B.A.S Roopa Devi, Dr.J.V.R Murthy &Dr.G.Narasimha, 'Secure Zone Based Routing Protocol for Mobile Adhoc Networks',pp.839-846,2013.

[4] Z.Zhi&Y.K. Choong, 'Anonymizing Geographic Ad Hoc Routing for Preserving Location Privacy', Proc. Third Int'l Workshop Mobile Distributed Computing (ICDCSW), pp.646-651, 2010.

[5] X. Wu, 'AO2P: Ad Hoc On-Demand Position-Based Private Routing Protocol', IEEE Trans. Mobile Computing, vol.4, Issue.4, pp.335-348, July/Aug.2005.

[6] Sanjay K. Dhurandher, 'FACES: Friend-Based Adhoc Routing using Challenges to Establish Security in MANETs Systems', vol.5, Issue.2, pp.176-188, 2011.

[7] Ruchigupta, 'A Survey of Energy Efficient Location Based Multipath Routing in MANETs',International Journal of Computer Applications, vol.59, no.11, pp.42-46, 2012.

[8] Mallikarjun B. Channappagoudar&PallapaVenkataram, 'Mobile Agent Based Node Monitoring Protocol for MANETs', IEEE National Conference on Mobile Computing, pp.1-5, 2013.

[9] Karim El Defrawy, & Gene Tsudik, 'ALARM: Anonymous Location Aided Routing in suspicious MANETs', IEEETransaction on Mobile Computing, vol.10, Issue.9, pp.1345-1358, 2011.

[10] Elhadi M. Shakshuki, Nan Kang,&Terek R. Sheltami, 'EAACK-A Secure intrusion-Detection System for MANETs', IEEE Transaction Industrial Electronics,vol.60,Issue.3,pp.1089-1098, 2013.

[11] Hung-Min Suna, Chiung-Hsun Chena, Ling-Chun Hsua& Yao-Hsin Chen, 'Reliable data transmission against packet dropping misbehavior in wireless ad hoc networks',IEEE International Conference on Wireless Mobile and Computing,pp.419-424,2011.

[12] JiajiaLui, Xiaohong Jiang, Hiroki Nishiyama&Neikato, 'Throughput Capacity of MANETs with Power Control and Packet Redundancy',vol.12,Issue.6,pp.3035-3047, 2013.

[13] Hanan Saleet, Rami Langar, KshirasagarNaik, RaoufBoutaba, Amiya Nayak&NishithGoel, 'Intersection-Based Geographical Routing Protocol for VANETs: A Proposal and Analysis',IEEE TransactionsonVehicularTechnology,vol.60,Issue.9,pp.4560-4574, 2011.

[14] Marcin Poturalski,PanosPapadimitratos& Jean-Pierre Hubaux,'Formal Analysis of Secure Neighbor Discovery in Wireless Networks', IEEETransactions on Dependable and Secure Computing,vol.10,Issue.6,pp.355-367,2013.

[15] Seon Yeong Han&Dongman Lee,'An Adaptive Hello Messaging Scheme for Neighbor Discovery in On-Demand MANET Routing Protocols', vol.17, Issue.5, pp.1040-1043, 2013.

[16] Adnan Abu-Mahfouz& Gerhard P. Hancke, 'Distance Bounding: A Practical Security Solution for Real-Time Location Systems', IEEE Transactions on Industrial Informatics,vol.9,Issue.1,pp.16-27,2013.

[17] Jie Yang, Yingying (Jennifer) Chen, Wade Trappe& Jerry Cheng, 'Detection and Localization of Multiple Spoofing Attackers in Wireless Networks', IEEETransactions on Parallel and Distributed System,vol.24,Issue1,pp.44-58,2013.

[18] Vinoth Kumar,K & Rajaram,A, 'Energy Efficient and Node Mobility based Data Replication Algorithm for MANETs', International Journal for Advance Research in Engineering and Technology(IJARET), vol.2, Issue.5, pp.1-4,2014.

[19] Raquel Lacuesta, Jaime Lloret, Miguel Garcia & Lourdes Pen alver,'A Secure Protocol for Spontaneous Wireless Ad Hoc Networks Creation',IEEE Transactions on Parallel and Distributed Systems,vol.24,Issue.4,pp.629-641,2013.

[20] Mohammed Erritali, Oussam a Mohamed Reda&Bouabid El Ouahidi, 'IJARCSSE: UML Modelling of Geographic Routing Protocol 'GPSR' for its integration into the Java Network Simulator', 2012.

[21] Chia-Mu Yu, Yao-Tung Tsou, Chun-Shien Lu&Sy-Yen Kuo,'Localized Algorithms for Detection of Node Replication Attacks in Mobile Sensor Networks',IEEE Transactions on Information Forensics and Security, vol.8,Issue.5,pp.754-768, 2013.

[22] Uvaraj,S & Suresh,S, 'Node Selection in P2P Content Sharing Service in Mobile Cellular Networks with Reduction Bandwidth', International Journal for Advance Research in Engineering and Technology(IJARET), vol.1, no.4, 2013.

[23] Daojing He, Chun Chen, Sammy Chan, Jiajun Bu & Laurence T. Yang,'Security Analysis and Improvement of a Secure and Distributed Reprogramming Protocol for Wireless Sensor Networks', IEEE Transaction on Industrial Electronics,vol.60,Issue.11,pp.5348-5354,2013.

[24] ShirinaSamreen& G. Narasimha, 'An Efficient Approach for the Detection of Node Misbehaviour in a MANETs based on Link Misbehaviour', IEEE3rd International Advanced Computing Conference,pp.588-592,2012.

[25] Jiajia Liu,Xiaohong Jiang, HirokiNishiyama&Nei Kato, 'On the Delivery Probability of Two-Hop Relay MANETs with Erasure Coding',IEEE TransactiononCommunications,vol.61,Issue.4,pp.1314-1326, 2013.

[26] KassemFawaz& Hassan Artail, 'DCIM: Distributed Cache Invalidation Method for Maintaining Cache Consistency in Wireless Mobile Networks', IEEE Transaction on Mobile Computing, vol.12, Issue.4, pp.1314-1326, 2013.

[27] Shakeela Attikeri & Preeti Patil, 'Rebroadcast Protocol based on Neighbour Coverage to Reduce Routing Overhead in MANETs', International Journal for Advance Research in Engineering and Technology(IJARET),vol.2, Issue.1,pp.16-21,2014.

[28] Peng Zhao, Xinyu Yang, Wei Yu &Xinwen Fu, 'A Loose Virtual Clustering based Routing for Power Heterogeneous MANETs',IEEE Transaction on Vehicular Technology,vol.62, Issue.5,pp.2290-2302,2011.

[29] KannanGovindan&PrasantMohapatra, 'Trust Computations and Trust Dynamics in MobileAdhocNetworks: A Survey',vol.14,Issue.2,pp.279-298,2012.

[30] JanuszKusyk, JianminZou, Stephen Gundry, CemSafakSahin& M. mitUyar, 'Metrics for performance evaluation of self-positioning autonomous MANET nodes', IEEE Sarnoff Symposium, pp.1-5, 2012.

[31] Quansheng Guan, F. Richard Yu, Shengming Jiang & Victor C. M. Leung, 'Joint Topology Control and Authentication Design in Mobile Ad Hoc Networks with Cooperative Communications', IEEETransactiononVehicularTechnology,vol.61 ,Issue.6,pp.2674-2685,2012.

[32] Aldar C-F. Chan, 'Distributed Private Key Generation for Identity Based Cryptosystems in Ad Hoc Networks',IEEE Transactions on Wireless Communication,vol.1,Issue.1,pp.46-48,2012. 2012.

[33] Yingbin Liang, H. Vincent Poor& Lei Ying, 'Secrecy Throughput of MANETs Under Passive and Active Attacks',IEEE transactions on Information Theory, vol.57,Issue.10,pp.6692-6702, 2011.