International Journal of Advanced Computer Research (ISSN (print): 2249-7277 ISSN (online): 2277-7970)
Volume-4 Number-3 Issue-16 September-2014

Secure Geographical routing in MANET using the Adaptive Position Update

Aruna Rao S.L[1], K.V.N.Sunitha[2]

Abstract

MANETs are infrastructure free network, hence are mostly vulnerable to attacks and maintaining the anonymity of the nodes is also becoming a major concern. Most of the existing geographical routing methodology in Mobile Ad Hoc Networks (MANET) does not include any position update mechanism for anonymous mobile nodes. In this paper, we propose a secure geographical routing which uses an adaptive position update technique for MANET. When source wants to transmit the data to destination, it establishes a secured geographical route using group signature. Then a position update technique is used to dynamically adjust the position of nodes based on mobility and network forwarding patterns. The malicious node detection technique is used to detect the malicious node. By simulation results, we show that the proposed technique reduces packet dropping and enhances the packet delivery ratio.

Keywords

MANET, SGRAPU, PRISM, Network Simulator, Performance Metrics.

1. Introduction

Mobile Ad hoc Networks are collection of mobile terminals or nodes, allowing no stationary infrastructure and centralized administration. Since the last few decades, MANET has become the thrust area for researchers. MANET is variety of various cooperative mobile terminals and it is an autonomous system. Mobile Ad Hoc Network is not only a self organizing but also a self-configuring network. There are two types of mobile wireless networks. One is infrastructure networks i.e. Base Stations and second one is wireless network called as infrastructure less mobile network.

Manuscript received August 14, 2014.

K.V.N.Sunitha, Principal, BVRIT Hyderabad College of Engineering for Women,Rajiv Gandhi Nagar, Nizampet Road, Bachupally ,Hyderabad, India.

Aruna Rao S.L, Associate Professor, IT Department,BVRIT Hyderabad College of Engineering for Women,Rajiv Gandhi Nagar, Nizampet Road, Bachupally, Hyderabad, India.

Self-organizing and self-configuring network communicates with the nearest base station which lies within the range. One of the commonly known applications includes office Wireless Local Area Networks. Infrastructure less mobile network are commonly known as an Ad hoc Network due to mobile infrastructure, where all nodes move freely, topology may change rapidly and is typically unpredictable over time, and nodes have to form their own mutual infrastructures [1][2][3].

The applications of MANET includes emergency search, military battlefields, Disaster relief applications, interactive lectures or conferences, intelligent buildings, logistics and rescue locations etc which requires quick deployment and active re-configuration. Finding the path between the two hosts in adhoc network in a routing protocol is very staggering tasking due to their highly dynamic topology, absence of centralized administration. In adhoc networks mobility, bandwidth, and resource constraint, hidden and exposed terminal problems are considered while designing routing protocols [3][4].
The primary challenge of MANET based applications are trustworthiness because these applications depends on a multitude of factors. Providing an efficient route establishment between a pair of nodes is the primary goal of an adhoc network and the route construction should be done with a minimum of overhead and bandwidth consumption. Multicasting plays a major role for communication in MANET, wherein tasks for a particular group are often deployed. To perform multicasting effectively, a group having one or more group members is constructed and an address called multicast address is assigned to each of these groups. In MANET, members of the group spread randomly and move frequently in the entire network, which causes more difficulty in packet delivery and group maintenance [3][4].

1.1 Geographical routing in MANET

Geographic routing is becoming one of the attractive routing in MANET, because the nodes know their own locations (e.g., using GPS) as it only requires estimates of the locations of its immediate neighbors and of the destination node in order to forward a message. A node can estimates of its neighbors locations quite easily when the nodes in the network are moving [4][5][6].

By using the Position-based routing algorithms we can eliminate some of the limitations of topology-based routing by using additional information. Position based routing means forwarding packets to the destinations position or nearer to the position. Each node requires information of the position of the participating nodes to be available. Every node can estimate its own location with the help of GPS or any other type of positioning service. To determine the position of the destination we use a location service GPS. GPS takes the help of satellites and use them as reference points to effectively calculate the location/positions of ground nodes.There are many real world applications of GPS to name a few: location estimation, tracking, navigation mapping and providing timing services [4][5][7].

The main advantage of using the Geographical routing is, we can avoid the flooding of control traffic. Information an intermediate node needs is its own position as well as the positions of its neighbouring nodes to make a message forwarding decision. The message is send to the node which is geographically close to the destination. We must know the information about the geographical location of each destination to implement a position-based routing protocol. Each node can be able to estimate its own location with the help of the Global Positioning System (GPS), or its relative position by using GPS free positioning methods.

1.2 Secure Geographical Routing

In the Geographical routing trusting the neighbouring node is an important thing because there is an implicit trust-your-neighbour relationship in which all the neighbouring nodes behave properly. In the Geographical routing, the forwarding decision is based on Location Information and the location information may be hacked by the hackers, to know all the details. It is necessary to secure the location information that is exchanged between the nodes.

The attacker enters into the real networks and they may try to change the MANET by manipulating the messages. Hence, having a routing protocol which is secure is nontrivial. Recently, several secure ad hoc routing protocols have been proposed for secure geographical routing with the aim of preventing various possible attacks.

In Geographical routing protocols routing tables are not stored in nodes that are kept up-to date via message exchanges, as there are significant privacy and security concerns regarding their location service that integrates tracking and navigation capabilities.

In general attackers are divided into two types, one is malicious users and second one is compromised users. An attacker who is from outside and there is no valid shared cryptographic key information is called as malicious users. An insidier who is forced to compromise is capable of launching many kinds of attacks which hardly gets detected by other entities. Several attacks can be launched either by a compromised or by a malicious against the position-based routing protocols in MANETs.
Some of the well knows attacks are:

1.2.1 Location table tampering attack: Here the attacker can change the information stored in the location table. This attack includes the physical deletion, alteration or falsification of information stored in location tables in a node. The location table tampering attack is practical against any position-based routing protocols.

1.2.2 Message dropping attack: In this attack the attacker intentionally drops some (or all) control or data packets. Originally nodes in MANET operate as both end hosts and routers, attacks like message dropping can paralyze the network completely as the number of attacker's increase.

1.2.3 Message tampering attack: In this attack, the attackers change the content in any packet. Example of these attacks are (i) impersonating other nodes, and (ii) relaying or generating packets with altered contents.

1.2.4 Message replay attack (e.g., wormhole): In this attack, the attackers snoop the packets and replay those packets again later.

1.2.5 Blackmail attack: Causing the false identification of a good node as a bad one. This kind of attack generally occurs in networks where there is a possiblity of having a feedback with negative reputation [7][8][9][10].

1.3 Problem Identification

The approach which is proposed in [13] is an on-demand location-based anonymous MANET routing protocol (PRISM) that achieves privacy and security against both outsider and insider adversaries. It totally relies on group signatures in order to authenticate nodes, and also ensure integrity of routing messages while preventing node tracking. It is operational not only with any group signature scheme but also with any location-based forwarding mechanism.

Following are the drawbacks observed in the above approach:

1. This scheme does not dynamically adjusts the frequency of position updates in geographical routing.
2. In this scheme there is no method for malicious node detection so we cannot delete the malicious node from the network.

2. Related Work

Karim Defrawy et al., [11] have proposed a protocol for Anonymous Location-Aided Routing in MANETS (ALARM) that demonstrates the feasibility of simultaneously obtaining, strong privacy, and security properties, with reasonable efficiency. Privacy here relates to anonymity of the node and its resistance to tracking. Although it might seem that their security and privacy properties contradict each other, they show that some advanced cryptographic techniques can be used to reconcile them. This protocol offers protection against both passive and active insider and outsider attacks.

Quanjun Chen et al., Salil S. Kanhere, and Mahbub Hassan, [12] have proposed Adaptive Position Update (APU) strategy for geographic routing, which dynamically adjusts the frequency related to position updates based on the mobility dynamics of the nodes and the forwarding patterns in the network. APU is based on two simple principles: (i) updations related to position of the nodes are done more frequently whose movements are harder to predict (and vice versa), and (ii) nodes which are closer to the forwarding paths update their positions more frequently (and vice versa).

Karim El Defrawy et al., [13] have proposed on-demand location-based anonymous MANET routing protocol (PRISM) that achieves privacy and security against both outsider and insider adversaries. The PRISM protocol which supports anonymous reactive routing in suspicious location-based MANETs relies on group signatures to authenticate nodes, ensure integrity of routing messages while preventing node tracking. This protocol operates not only with any group signature scheme but also with any location-based forwarding mechanism.

Erik Kuiper et al, [14] have proposed a geographical routing algorithm LAROD enhanced with a location service LoDiS, together shown to suit an intermittently connected MANET (ICMANET). Location dissemination takes time in ICMANETs LAROD as it is designed to be able to route packets with only partial knowledge of geographic position. Beaconless stratergy combined with position-based resolution of bids is used by LAROD to achieve a low overhead while forwarding packets. A local Database related to locations of a node is maintained by LoDiS which is updated using broadcast gossip combined with routing overhearing.

Vivek Patha al., [15] have proposed a geographical secure path routing, an infrastructure free geographic routing protocol, that is resilient to disruptions caused by malicious or faulty nodes. Their protocol also authenticates the routing paths taken by individual messages. Geographical secure path routing protocol requires associative cryptographic one-way hash functions for security. These hash functions are derived from the discrete algorithm problem which uses expensive modular arithmetic. This makes their protocol unsuitable for power limited devices.

Vivek Pathak et al., [16] have proposed to secure location aware services over vehicular ad-hoc networks (VANET) with our geographical secure path routing protocol (GSPR). This protocol is an infrastructureless geographic routing protocol, which is very resilient to disruptions caused by malicious or faulty nodes. Authentication related to geographic locations of the anonymous nodes is necessary in order to provide location authentication and location privacy simultaneously. Their protocol also authenticates the routing paths taken by individual messages.

3. Proposed solution

3.1 Overview

In this paper, we propose a secure geographical routing using the adaptive position update technique in MANET. When source wants to transmit the data to destination, it establishes a secured geographical route using group signature. Then a position update technique is used to dynamically adjust the position of nodes based on mobility and network forwarding patterns. The malicious node detection technique is used to detect the malicious node.

3.2 Secured Routing

In this phase, we establish a secured route between S and D for performing data transmission. The secured routing is done using group signatures which are appealing building block for anonymous MANET routing protocols. Message can be signed by any member of a large and dynamic group, thus producing a group signature. It can be verified by anyone who has a copy of a constant-length group public key.

Let the source and destination be denoted as S and D respectively. Let R_RQ and R_RP be the route request and reply respectively. Let c_s and c_d be the coordinates of the source and destination respectively. Let r_s and r_d be the radius of the source and destination respectively.

(1) S broadcasts R_RQ message with destination address (A_D), public key (K_{pu}), time stamp (TS) and source group signature (GS_s) to its neighbour nodes (N_i). The format of route request message is shown below in table1.

Table 1: Format of Route Request

Source Area (A_S) (c_s, r_s)	Destination Area (A_D) (c_d, r_d)	Public Key (K_{pu})	Time Stamp (TS)	Source Group Signature (GS_s)

Note: S initiates the node search within the smaller radius and even if no R_RP is received with a time t, it increases the radius and transmits another R_RQ.

(2) Each N_i upon receiving R_RQ verifies TS and then if R_RQ is within A_D.

i) If TS = invalid
Then
N_i drops the R_RQ
Else
N_i verifies whether it has already processed similar R_RQ by estimating hash value of R_RQ H (R_RQ) and comparing it with the request message already stored in route cache.
End if

ii) If R_RQ is not within A_D
Then
N_i caches H (R_RQ) and rebroadcasts the R_RQ
Else
N_i verifies GS_s
If GS_s = valid
Then
N_i stores the R_RQ
Else
N_i discards R_RQ
End if

(3) D then generates R_RP with H (R_RQ), random session (K_s), destination location (c_d, r_d) and destination group signature (GS_d) and broadcasts it. The format of R_RP is shown below in table 2.

Table 2: Format of Route Reply

H(R_RQ)	Destination Area (A_D) E(K_{pu}) {c_d, r_d}	Session Key (K_s) E (K_{pu}) {(K_s)}	Time Stamp (TS)	Destination Group Signature (GS_d)

The destination area and session key are encrypted using temporary K_{pu}. This prevents eavesdropping effect.

(4) Each N_i upon receiving R_RP performs the following action:
If N_i (Not cached the respective H (R_RQ)) || (processed the similar R_RP)
Then
N_i drops the R_RP and generates the new active route entry and re-broadcasts the R_RP.
Else
R_RP is forwarded towards S
End if

The new generated route details includes H(R_RQ), H(R_RP) and TS.

(5) S upon receiving R_RP verifies the TS, A_D and GS_d.
If it is invalid
Then
R_RP is discarded and S waits for another R_RP.
Else
S performs routing in the established route.
End if

(6) Each S-D data includes the < H (R_RQ), H (R_RP)> as route identifier. On the other hand, D-S uses <H (R_RP), H (R_RQ) > is used as route identifier. The data is encrypted with K_s.

3.3 Position Adjustments of Nodes

In this phase, the following two mutually exclusive rules are used that dynamically adjusts the position of nodes based on mobility and network forwarding patterns.

1) Mobility Prediction
2) On-Demand Learning

Mobility Prediction

Let V_i and A_i be the predicted and actual location of N_i. This involves beacon generation rate adjustment to the frequency with which the nodes alter its movement features i.e. velocity (q) and location (v). These features are added to the beacon broadcast message when the node broadcasts the request messages to its neighbors.

Note: Only nodes with high mobility need to frequently update its position to its neighbors.

Each N_i upon receiving beacon update from its neighbor nodes ($Neigh_i$) stores q_i and v_i and tracks the v_i of $Neigh_i$ position in periodic manner.

Based on x_i, N_i verifies whether $Neigh_i$ is within the transmission range and updates the neighbor nodes list.

If (V_i~ A_i) > threshold
Then
N_i transmits the next beacon message
End if

Let t_f and t_{cu} be the last beacon broadcast time and current time. Let (X^i_v, Y^i_v) be the location coordinates of N_i at t_f. Let (Q^i_x, Q^i_y) be the velocity of N_i along x and y axes at t_f. Let (X^i_p, Y^i_p) be the predicted position of N_i at t_{cu}. Let (X^i_{ac}, Y^i_{ac}) be the actual location of N_i obtained using GPS.

The position of Ni is predicted based on q_i and v_i along x and y axes at time t as follows:

$$\mathbf{X^i_p = X^i_v + (t_f - t_{cu}) * Q^i_x} \quad \textbf{(1)}$$

$$\mathbf{Y^i_p = X^i_v + (t_f - t_{cu}) * Q^i_y} \quad \textbf{(2)}$$

N_i estimates the deviation D_i using the following Equation (3).

$$\mathbf{D_i} = \sqrt{(X^i_{ac} - X^i_p)^2 + (Y^i_{ac} - Y^i_p)^2} \quad \textbf{(3)}$$

If D_i > threshold
Then
N_i broadcasts a new beacon message with its current v_i and q_i
End if

Figure 1 demonstrates the mobility prediction technique.

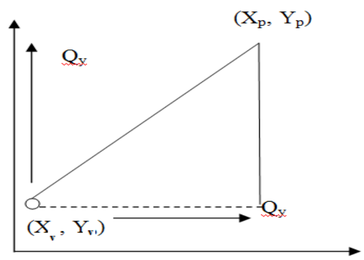


Figure 1: Mobility Prediction

On-Demand Learning:

When MP rule fails, the ODL rule is applied. This technique accurately maintains the local topology of the network, where the data forwarding activities are currently processed.

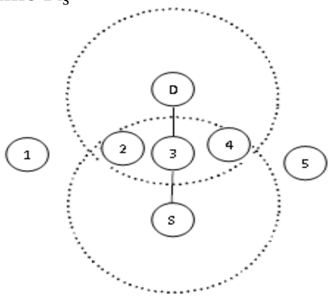
Consider that a data packet DP to be transmitted from S to D. DP includes location information of D.

1) When any N_i overhears a transmitted data from a new $Neigh_i$, it broadcasts the beacon message.
   Note the following:
   - N_i waits for small time t prior sending beacon message to prevent collision.
   - New $Neigh_i$ means that the node detail does not exist in route cache.

2) Also N_i verifies if the destination node is within the transmission range.
   If D exists within the transmission range
   Then
   D is added to the neighbour node list if does not exists already.
   End if

The Neighbour list is maintained at each active node with respect to network traffic. However the inactive nodes maintain the basic neighbour list alone. This on-demand learning process guarantees the establishment of alternate routes without additional delays for high mobility nodes.

After route discovery, the data forwarding between source and destination is encrypted and authenticated using one-time K_s



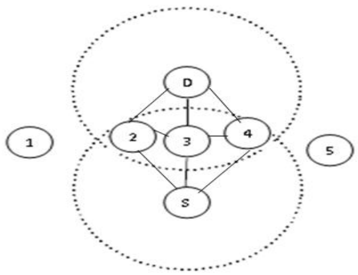


Figure 2: On-demand Learning Technique

Figure 2 illustrates the data transmission from S to D. Possible path from S to D = S $\rightarrow N_3 \rightarrow$ D. When S transmits DP to D, N_2 and N_4 receives DP from S. As S is neighbour of N_2 and N_4, N_2 and N_4 transmits beacon back to S. Thus links SN_2 and SN_4 is discovered. Similarly, when N_3 forwards DP to D, links N_3N_2 and N_3N_4 are discovered.
Note: Though N_1 and N_5 receive the beacons from N_2 and N_4, beacon messages are not sent back as N_1 and N_5 are out of forwarding path.
After route discovery, the data forwarding between S and D is encrypted and authenticated using one-time K_s.

3.4 Malicious Node Detection

Following the route construction, when any attack occurs, then the malicious node is detected using the following detection technique.

Each N_i listens to the neighbour nodes transmission information to detect malicious nodes. The information includes periodic beacon's inconsistencies, correctness of geographically routed messages and reverse source routed responses.

If N_i detects the malicious nodes
Then
    It warns the neighbouring nodes through
    Periodic beacon
End if

The following two validations are performed for malicious node detection

Validating Beacon

1) When any N_i receives beacons from neighbouring nodes, it is stored in local cache.
2) When any N_i launches false location attacks, it is detected using range constraint R.
3) In general, all the nodes reports it location and geographic hash of two-hop neighbours.
4) Each N_i constructs the mapping that includes the location details received from each neighbour.
   i) Minimal location inconsistencies are ignored as location error.
   ii) Maximum location inconsistencies cause the node to decide that its one-hop neighbourhood contains malicious nodes and considered to be worst neighbourhood.
5) Nodes in worst neighbourhood does not forward message, however proceeds to transmit the beacon in order to propagate geographic hashes and malicious node information.

Forwarding validation

Consider figure 2 Let S, N_3 and D be successive hops on routing path. All the transmission made by N_3 is received by S as it is within one-hop. Thus S can detect if N_3 fails to forward the message to next-hop. Similarly S can verify the overheard next-hop transmission for malicious payload modification.
If N_3 and D are malicious, N_3 can forward the message to D and does not report malicious forwarding by D. This is detected by N_4 in one-hop distance. Thus on malicious node detection, S finds another route to D. S also verifies the message integrity and feasibility of routing paths by validating the geographic location list for maximum transmission limit. Those messages that violate R are dropped and the previous hop nodes are marked as malicious.

Advantages of this approach

- Provide the integrity and confidentiality against both outsider and insider adversaries.
- Secure geographical routing with the group signature.

- It will reduce the update cost and improve the routing performance in terms of packet delivery ratio and average end-to-end delay.

4. Simulation Results

4.1 Simulation Model and Parameters

The Network Simulator (NS2) [17], is used to simulate the proposed architecture. In the simulation, the mobile nodes move in a 500 meter x 500 meter region for 50 seconds of simulation time. Transmission range of all nodes in the network is same and is 250 meters. Constant Bit Rate (CBR) is used as simulation traffic.

The simulation settings and parameters are summarized as follows.

Table 3: Simulation Parameters

No. of Nodes	20,40,60,80,100
Area Size	500 X 500
Mac	IEEE 802.11
Transmission Range	250m
Simulation Time	50 sec
Traffic Source	CBR
Packet Size	512
Sources	4
Attackers	2
Nodes Speed	5,10,15,20,25m/s

4.2 Performance Metrics

The proposed Secure Geographical routing in MANET using the Adaptive Position Update (SGRAPU) is compared with the PRISM technique [13]. The performance of the proposed protocol is evaluated mainly, according to the below mentioned metrics.

- **Packet Delivery Ratio/ Throughput:** It is the ratio between the number of packets received and the number of packets sent.
- **Network Overhead**: It refers the number of routing overhead packets received by the receiver.
- **Total Delay** : It is the amount of time taken by the nodes to transmit the data packets.

4.3 Results

Simulation is carried out by increasing number of nodes by 20, 40, 60, 80 &100. Performance analysis is done on 2 criteria

a) Based on Number of Nodes
b) Based on speed of the nodes

Snapshot for simulation of 20 nodes in the network is shown below.

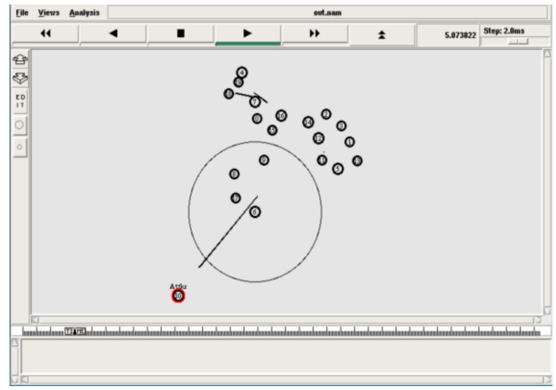


Figure 3: Simulation of 20 nodes

1) Based on Nodes

In our first experiment we vary the number of nodes as 20,40,60,80 and 100.

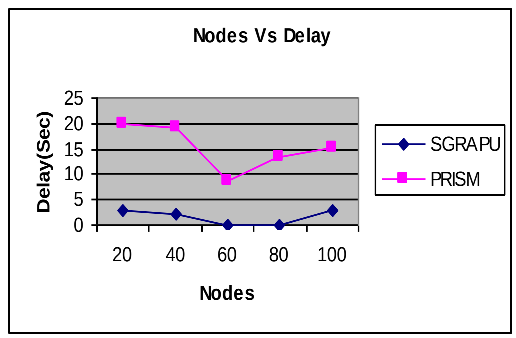


Figure 4: Nodes Vs Delay

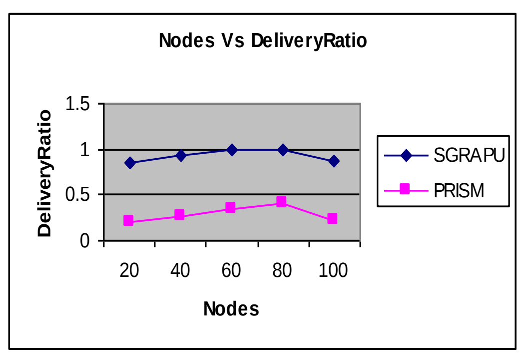


Figure 5: Nodes Vs Delivery Ratio

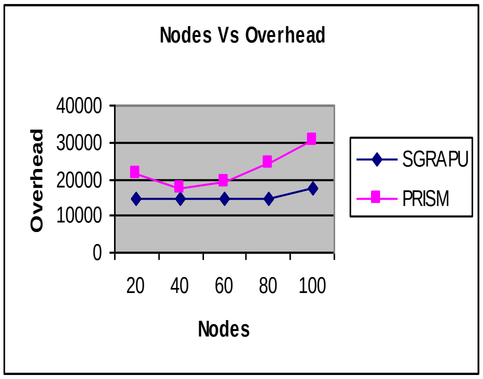


Figure 6: Nodes Vs Overhead

Figure 4 shows the delay of SGRAPU and PRISM techniques for different number of nodes scenario. We can conclude that our proposed SGRAPU approach has 91% less delay than PRISM approach.

Figure 5 shows the delivery ratio of SGRAPU and PRISM techniques for different number of nodes scenario. We can conclude that the delivery ratio of our proposed SGRAPU approach has 70% higher than PRISM approach.

Figure 6 shows the overhead of SGRAPU and PRISM techniques for different number of nodes scenario. We can conclude that the overhead of our proposed SGRAPU approach has 30% less than PRISM approach.

2) Based on Speed

In our second experiment we vary the nodes speed as 5,10,15,20 and 25m/s.

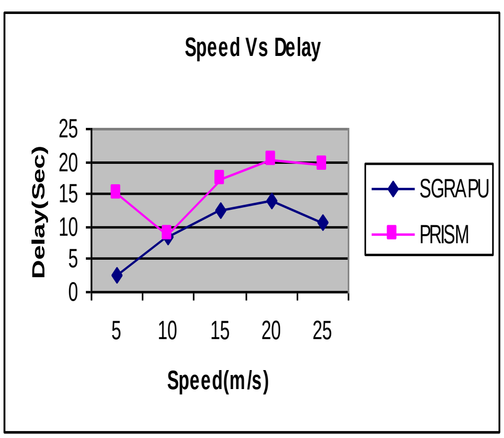


Figure 7: Speed Vs Delay

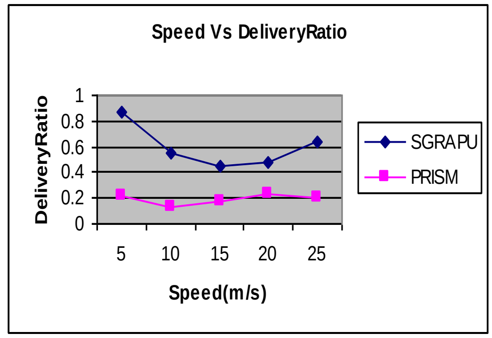


Figure 8: Speed Vs Delivery Ratio

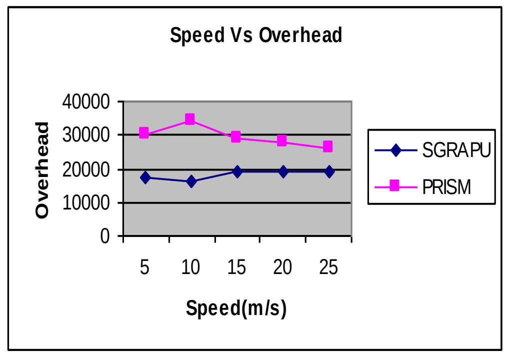


Figure 9: Speed Vs Overhead

Figure 7 shows the delay of SGRAPU and PRISM techniques for different speed scenario. We can conclude that the delay of our proposed SGRAPU approach has 38% less than PRISM approach.

Figure 8 shows the delivery ratio of SGRAPU and PRISM techniques for different speed scenario. We can conclude that the delivery ratio of our proposed SGRAPU approach has 67% higher than PRISM approach.

Figure 9 shows the overhead of SGRAPU and PRISM techniques for different speed scenario. We can conclude that the overhead of our proposed SGRAPU approach has 37% less than PRISM approach.

5. Conclusion

MANET consists of dynamic collection of nodes with rapidly changing multihop topologies where nodes move freely. Effective delivery of packets at proper location is one of the major challenges faced in such kind of infrastructure-less network. In this paper, we have proposed a secure geographical routing using the adaptive position update technique in MANET. When source wants to transmit the data to destination, it establishes a secured geographical route using group signature. Then a position update technique is used to dynamically adjust the position of nodes based on their mobility and network forwarding patterns. Paper also incorporates malicious node detection technique which is used to detect the malicious node. By simulation results, we have shown that the proposed technique effectively reduces packet dropping and enhances the packet delivery ratio.

References

[1] Umang Singh, "Secure Routing Protocols In Mobile Adhoc Networks-A Survey And Taxanomy", International Journal of Reviews in Computing, Volume 7, September 2011.

[2] Papadimitratos, Panagiotis, and Zygmunt J. Haas. "Securing mobile ad hoc networks." Handbook of Ad Hoc Wireless Networks (2002): 665-671.

[3] Sridhar K N and Mun Choon Chan, "Channel-aware Packet Scheduling for MANETs", International Symposium on a world of wireless networks IEEE, 2008.

[4] Turkan Ahmed Khaleel and Manar Younis Ahmed, "The Enhancement of Routing Security in Mobile Ad-hoc Networks", International Journal of Computer Applications (0975 – 888), Volume 48– No.16, June 2012.

[5] Joo-Han Song, Vincent W.S. Wong and Victor C.M. Leung, "Secure position-based routing protocol for mobile ad hoc networks", Elsevier, Ad Hoc Networks Journal, vol. 5, issue 1, pp. 76-86, January 2007.

[6] Sanjeev Sharma and Sanjay Singh, "A Survey Of Routing Protocols And Geographic Routing Protocol Using Gps In Manet", Journal of Global Research in Computer Science, Volume 3, No. 12, December 2012.

[7] Joo-Han Song, Vincent W.S. Wong, and Victor C.M. Leung, "A Framework of Secure Location Service for Position-based Ad hoc Routing", In: Proceedings of the 1sr ACM international workshop on Performance evaluation of wireless ad hoc, sensor, and ubiquitous networks, Venezia, Italy, pp, 99-106 (2004).

[8] Dinesh Ramasamy and Upamanyu Madhow, "Geographic Routing in Large-Scale MANETs", IEEE International Symposium on Information Theory Proceedings 2012.

[9] Tim Leinmuller, Christian Maihofer, Elmar Schoch and Frank Kargl, "Improved Security in Geographic Ad hoc Routing through Autonomous Position Verification", ACM,VANET'06 Proceedings of the 3rd International workshop on Vehicular ad hoc networks, Pages 57-66, 2006.

[10] M.Shobana, R.Saranyadevi and Dr.S.Karthik, "secure data delivery using geographic multicast routing", International Journal of Advanced Research in Computer Engineering & Technology (IJARCET) Volume 1, Issue 7, September 2012.

[11] Karim El Defrawy, and Gene Tsudik, "ALARM: Anonymous Location-Aided Routing in Suspicious MANETs", IEEE Transactions on Mobile Computing, VOL. 10, NO. 9, September 2011.

[12] Quanjun Chen, Salil S. Kanhere, and Mahbub Hassan, "Adaptive Position Update for Geographic Routing in Mobile Ad-hoc Networks", IEEE, Mobile Computing, IEEE Transactions on (Volume:12 , Issue: 3), March 2013.

[13] Karim El Defrawy, and Gene Tsudik, "Privacy-Preserving Location-Based On-Demand Routing in MANETs", IEEE Journal On Selected Areas In Communications, Vol. 29, Issue10, December 2011.

[14] Erik Kuiper and Simin Nadjm-Tehrani, "Geographical Routing with Location Service in Intermittently Connected MANETs", IEEE, Vehicular Technology, IEEE Transactions on (Volume: 60, Issue: 2), February 2011.

[15] Vivek Pathak, Danfeng Yao Liviu Iftode, "Securing Geographical Routing in Mobile Ad-hoc Networks", Rutgers University Computing Coordination Council (CCC) Pervasive Computing Initiative Grant, 2008, NSF Grant CNS-0520123.

[16] Vivek Pathak, Danfeng Yao and Liviu Iftode, "Securing Location Aware Services Over VANET Using Geographical Secure Path Routing", IEEE International Conference on Vehicular Electronics and Safety, 2008. ICVES 2008.

[17] Network simulator: http:///www.isi.edu/nsnam/ns

Dr. K.V.N. Sunitha is currently working as Principal for BVRIT Hyderabad college of Engineering for Women. The author has a total of 22 years of teaching experience. She has completed her BTech (ECE) in the year 1988, MTech (CSE) in the year 1993 and Ph.D in the year 2006. She has received "Best computer Science engineering Teacher award for the year 2007" by Indian Society for Technical Education ISTE. Her autobiography was included in "Marquis Who is Who in the World " , 28th edition 2011. She has authored three text books, "Programming in UNIX and Compiler design"- BS Publications & "Formal Languages and Automata Theory" by Tata McGraw Hill & "Theory of Computation" by TMH in 2011.She has developed web content for compiler design subject for gradience portal in collaboration with Aho Ullman, Professor, Stanford University (USA). Her areas of research include Natural language processing, Speech Processing, Network & web Security. She has published more than 65 papers in International & National Journals and conferences. She is a reviewer for many national and International Journals. She is fellow of Institute of engineers, Sr member for IEEE & International association CSIT, and life member of many technical associations like CSI and ACM.

Aruna Rao S.L. is currently working as Associate Professor in Department of Information Technology, BVRIT Hyderabad college of Engineering for Women. The author has a total of 10 years of teaching experience. She has completed her BTech (Information Science) in the year 2001 and MTech (Networking and Internet Engineering) in the year 2006 and is currently pursuing her research in the area of adhoc networks. She is a member of technical associations like CSI, ACM.