IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661, p- ISSN: 2278-8727Volume 16, Issue 3, Ver. V (May-Jun. 2014), PP 75-82
www.iosrjournals.org

PARS: Position based Anonymous Routing Scheme in MANETs

Remya S, Lakshmi K S
MTech, Network Engineering, Department of IT, Rajagiri School of Engineering
Assistant Professor Department of Information Technology, Rajagiri School of Engineering

Abstract: *Mobile Ad hoc Networks (MANET) comprises of self-organizing autonomous mobile nodes. MANETs are open and decentralized. Therefore they are vulnerable to malicious entities. MANETs are multi-hop wireless network where all nodes supportively maintain network connectivity without a centralized infrastructure. Since MANETs are infrastructure less and independent, the secure communication is the main issue. Therefore they are vulnerable to malicious entities. Here the location identity and traffic can be traced out by an outside observer. Anonymity means secure communications by hiding node identities and preventing traffic analysis attacks by outside observers. This paper proposes Position based Anonymous Routing Scheme in MANETs (PARS).Here the routing is based on Greedy Perimeter Stateless Routing Protocol. The objective is an anonymous routing protocol for the network. The proposed one is a zone based anonymous GPSR based protocol that can provide source, destination and route anonymity. Performance of the proposed system is compared with that of GPSR and AODV using Network Simulator.*

Index Terms: *Anonymous routing, position-based routing, random forwarder,zone partition.*

I. Introduction

Mobile Ad hoc Networks are collection of independent mobile nodes that can communicate by radio waves. It is an infrastructure less self-organizing network. The nodes that are in radio range can communicate by single hop or by multi hop with the help of intermediate nodes. The network is open and decentralized and fully distributed. So they are perfect choice for communication and information sharing. MANETs are susceptible to malicious entities that aim to alter and analyzed the traffic analysis by communication eaves dropping or attacking routing protocols.

MANETs are characterized by their distributed operation, multi hop routing, dynamic topology and shared physical medium. Nodes in a MANET are independently free to move in any direction. Due to the lack of a centralized coordinator security is the major concern here. Wireless communication can endure interferences or malicious interceptions; whereas multi-hop communication assumes that each node will perform properly its functions to support network services. Further, self-organization increases the complexity of security management operations as access control, node authentication, secure routing and cryptographic key distribution. There is no fixed infrastructure and the topology is frequently changing due to node mobility or environmental changes. Therefore, it is very hard to maintain a stable and efficient end-to-end route in an ad-hoc network.

Each node in MANET is energy constrained. There is verylimited physical security in MANET. The type of attacks can be Active attacks or Passive attacks. The common security issues are Passive attacks which include eaves dropping and information disclosure. Active attacks include Do Sand Data modification. There are other more specific problems with mobile ad hoc network such as vulnerability of channels and nodes, Byzantine black hole and Byzantine wormhole attack. The security issue also includes attacks that may inject erroneous routing information and diverting network traffic thus making routing inefficient. There are many methods to reduce the impact of these attacks, which include a secure routing using public and private key s to get a certification authority and use of digital signatures and prior it rust relationships.

Routing is the process of communication from one node to the other host in a network. Routing is the process off or warding packet towards its destination using most efficient path. Routing efficiency is measured in terms of Number of hops, traffic, security, etc. Routing protocols in MANETs are divided as reactive proactive and hybrid. Reactive Protocol maintains the routes in on demand manner. In route discovery phase it floods the route request (RREQ) packets throughout the network. Dynamic source Routing (DSR), ad hoc on-demand distance vector routing (AODV) are some of the examples of reactive protocols.

In proactive approach every node in the MANET continuously maintains the complete routing information of the entire network. This is accomplished by flooding network periodically with network status information. Global State Routing (GSR), Hierarchical State Routing (HSR) and Destination Sequenced Distance Vector Routing (DSDV) are some of the examples of proactive routing protocols. Hybrid protocols are those maintains the properties of both proactive and reactive approaches. Zone Routing Protocol (ZRP) is an example of this type protocol.ZRP divides the topologyinto zones and seek to utilize different routing protocols within and between the zones based on the weaknesses and strengths of these protocols. Intra-zone routing is done by a proactive protocol and inter-zone routing is done by a reactive protocol.

Position-based routing algorithms need information about the physical position of the nodes in the network. This routing procedure can reduce some of the limitations of topology-based routing. Each node having a GPS facility to trace its own position. Position based routing is mainly has location service that enables the sender to determine the packet destination location and forwarding strategy used to forward the packets. A forwarding strategy can be like Greedy forwarding, restricted directional flooding and Hierarchical routing. The routing scheme at each node is then based on the location of destination contained in the packet and the location of the forwarding node's neighbors. Security is a major concern in MANETs routing. MANETs are widely acceptable for different applications. Applications such as military and disaster management should need strong security features. They need anonymous routing protocols. They are essential in MANETs to provide secure communication. They provide security by hiding the node location and identities and preventing traffic analysis is attacks from outside observers. Anonymity means identity and location anonymity of data sources (i.e., senders) and destinations (recipients), as well as route anonymity [12] Identity and location anonymity means it is hard if possible for other nodes to obtain the real identities and exact locations of the sources and destinations. Route anonymityis that no one cannot trace a packet flow to its source or destination, and no node has information about identities and locations of intermediate nodes in that route. [2] Position based Anonymous Routing Scheme is an effective solution to counter intersection attacks and timing attacks. This canal so offer routing efficiency comparable to the greedy perimeter state less routing algorithm. Exiting anonymous routing protocols are depending on neither hop- by-hop encryption nor redundant traffic and produce high cost. These protocols are incapable to provide the source, destination, and route anonymity together. If attacker knows the source and the destination of the communication it will try to hack the message send by the source and if the attacker knows the route between the sources it is possible to hack the message by analyze the routing pattern through that communication.

Contributions inthe proposed paper are highlighted asfollows.

- The underlying routing protocol is GPSR. Changes are made to the routing of GPSR to provide anonymity in the network. Random forwarders are selected based on their distance to the receiver and the data packets are broadcasted through these forwarder nodes.
- Due to mobility of nodes the random forwarders are selected based on distance calculation on that instant.

Section II reviews related work on anonymous routing schemes for mobile ad hoc networks. Section III discusses the basic idea of Position based Anonymous Routing Scheme (PARS). Section IV gives the performance evaluation of PARS. Simulation is used to test the performance of PARS, and the settings and results of these experiments are in Section IV. Section V concludes the idea with future enhancements and research.

II. Related work

An ad hoc wireless network is a temporary and dynamic environment where a group of mobile nodes with radio frequency transceivers communicate with each other without the intervention of any centralized administration or established infrastructure. Because of limited transmission range and resource constraints of each mobile node the communication sessions between two nodes are usually established through a number of intermediate nodes, which are supposed to be willing to cooperate while forwarding the messages they receive to their destination. Unfortunately, some of these intermediate nodes might not be trustworthy and might be malicious, there by forming a threat to the security and/or confidentiality of the exchanged data between the mobile nodes. The data packet is protected by the encryption. The traffic analysis may reveal valuable information about end users and their relationships. Anonymous routing provides security and privacy against traffic analysis.

Anonymous routing protocol should support privacy of node identity from intermediate nodes, intruders and outsiders, privacy of node identity of intermediate nodes, location Privacy for source and destination nodes, hiding hop count information and route privacy that means adversaries cannot trace a packet from source to destination. Many anonymity routing algorithms are based on the geographic routing protocol (e.g., Greedy Perimeter Stateless Routing (GPSR)) that greedily forwards a packet to the node closest to the destination. The intermediate relay node selection makes them easy to trace source, destination and traffic.

Anonymity routing protocols in MANETs can be classified into two categories such as hop-by-hop encryption and redundant traffic. They provide anonymity at heavy cost due to their public-key-based encryption and redundant traffic-based routing. In addition, many approaches cannot provide all of the afore mentioned anonymity protections. For example, ALARM cannot protect the location anonymity of source and destination, SDDR cannot provide route anonymity, and ZAP only focuses on destination anonymity. Anonymous routing protocols in MANETs are based on GPSR algorithm that greedy forward the data packets to the node that is closer to the destination.

Anonymous Location- Aided Routing in MANETs (ALARM) based on proactive routing procedure. The location Announcement Message (LAM) from each node is flooded throughout the MANET. Each node can build a map for by using these LAM for anonymous route discovery. ALARM needs an off-line group manager (GM).To sets the underlying group signature scheme is the GMs duty. He registers all legitimate nodes as group members. The GM is responsible for opening the contested group signature and determining the signer in case of disputes. The GM has to handle joining of new members as well as cancellation of existing ones. The propagation of updated revocation information to all legitimate nodes is also needed in real-time. When a node wants to communicate to a location then it checks whether a node exist in that location based on LAM mapping. If it got a node like that then it sends that message to the destination. The message is encrypted by using Diffie-Hellman (DH) or RSA technique. [5]

PRISM is an anonymous location-centric on- demand routing protocol based on the AODV protocol, a secure group signature and location information. To produce the group signature, any member can sign the message. This can be verified by anyone who has the copy of group public key. The valid group signature indicates that the signer is a bona fide group member. To avoid the dispute a Group Manager (GM) has to open a group signature and identify the actual signer. In PRISM the source authenticates the destination and vice versa. Intermediate nodes do not have the location of the source or the destination. They are not authenticated. The communication between source and destination is encrypted and authenticated using a session key. The source broadcasts a route request (RREQ), it contains the location of destination, temporary public key PKTMP, time-stamp TSSRC and group signature. PRISM relies on group signatures to authenticate nodes and ensure integrity of routing messages. [14]

The ZAP protocol preserves destination anonymity through the use of anonymity zone (AZ), under which a destination is collocated with a number of other nodes. The idea is to create an AZ based on a carefully selected pseudo destination (PD). Mainly, the ZAP protocol has two distinct variants: one uses destination-based AZ, and the other uses route-based AZ. The real destination generates a PD, which has a random position not too far from that of the real destination. The PDs position is carried in request and data packets in the PD field. Therefore, the connection request does not have to carry the real identity of the destination, as it is not required for routing. This guarantees the destination anonymity, even if the source is compromised. In PD-ZAP, a packet will finally be received by a node that is closest to the PD. This node then acts as a proxy and broadcasts the received packet to all of its neighbors. In PD-ZAP, the position of the PD is also used as the session ID, according to which a node receiving a packet from the proxy knows whether it is the destination. For nodes that are within the proxy broadcast range, only the destination will be able to decrypt the packet using the established symmetric key. Other nodes simply drop the packet. During the same session, proxies can be different. [6]

This is because when different packets arrive at the D-AZ, the node that is closest to the PD may be different. In PD-ZAP, the distance between the PD and the real destination cannot be too large. So the anonymity set cannot be large. To address such a problem, we propose G-ZAP, which uses a relatively large D-AZ for improving destination anonymity. As the destination may not be able to receive the packet directly from the proxy, an approach similar to geo casting is applied on which a packet is locally flooded in a geographic area. In G-ZAP, a destination selects a circular area within which it is located as its D-AZ. The source then sends packets toward the center of this area. Information about the D-AZ, such as the position of the center and the radius, is carried by data packets for routing purposes.

Both PD-ZAP and G-ZAP build an AZ around the destination. This could generate a trade-off problem between the AZ size and the communication overhead within a hot region. This paper presents a strategy that creates an AZ along the forwarding path. This scheme makes it possible to obtain a larger AZ without incurring heavy communication load in a spot. This use a route with redundant hops to increase the size of AZ. We call this approach RR-ZAP. Like PD-ZAP, in RR-ZAP, a client (destination) creates a PD, to build a private route. Data packets are delivered toward the PD. They will finally be received by a proxy and are locally broadcast. RR-ZAP, which uses redundant routes to improve anonymity, can achieve a high packet delivery ratio and assure the highest anonymity. If the anonymity requirement is not high, PD-ZAP can be used, because it achieves efficient node anonymity and still achieves a good routing performance in many cases. G-ZAP has to trade the performance for anonymity.

SEAD protocol based on the DSDV-SQ version of the insecure DSDV ad hoc network routing protocol. Using SEAD, an attacker can’t create a valid advertisement

With larger (better) sequence number that it received. For advertisements sent using the largest received sequence number, attackers that do not plan cannot advertise a route shorter than the one it has heard. SEAD, designed within expensive crypto graphic primitives to each part of the protocol that is robust against multiple uncoordinated attackers creating in correct routing state in any other node, even in spite of active attackers or compromised nodes in the network. SEAD can provide better packet delivery ratio, although it does create more overhead in the network, both due to an increased number of routing advertisements it sends, and due to the increase in size of each advertisement due to the hash value on each entry for authentication.

Greedy Perimeter Stateless Routing (GPSR) is a simplified variant of the GFG protocol strictly employs the left hand traversal rule (the same definition is possible for the right hand rule as well). When face exploration encounters the next closer intersection the first edge of the next visited face is determined by simply choosing the edge lying incounterclockwise directionfromtheintersectededge. Obviously, when strictly applying the left hand rule in Fig.3, this method will visit the same face sequence as GFG, i.e.F1, F2, F1, F3, F4. This is due to the fact, that (in the depicted case) on encountering the next edge crossing with state point, then extra adjacent face which intersects with the open line segment can always be traversed by using the left hand rule and selecting from the crossing edge the next one in counter clockwise direction.[9]

III. Proposed system

The proposal of the anonymous routing is to ensure better security in the MANET network. The Position based Anonymous Routing Scheme (PARS) contains the following procedures

- Networkmodel
- Zonepartition
- Routing scheme
- Anonymity

In order to provide high anonymity protection (for sources, destination, and route) this paper proposes a Position based Anonymous Routing Scheme. PARS dynamically partitions a network field into zones and randomly choose nodes in zone as random forwarders to form a non-traceable anonymous route. In each stage of routing data sender or random forwarder partitions the network in to two in order to separate itself and the destination. It then randomly chooses a node in the other zone as then next forwarder node and uses the GPSR algorithm for the routing process. In each step, the data is broadcasted to n nodes in the destination zone, providing n-anonymity to the destination. In addition, it has a strategy to hide the data initiator among a number of initiators to strengthen the anonymity protection of the source. PARS are also resilient to intersection attacks and timing attacks this project analyze this scheme in terms of anonymity and efficiency. It also conducted experiments to evaluate the performance of this in comparison with other anonymity and geographic routing protocols. PARS provides route, source and destination anonymity. It uses randomized routing of one message copy to provide anonymity protection. This routing scheme is Resilience to intersection attacks and timing attacks. Over head similar to that of other GPSR based systems. The through put is higher than that of GPSR based systems.

A. Network model

Network model consider the random waypoint model and the group mobility model Network are classified into Zone. An anonymous routing protocol that can provide untraceable route that can ensure the anonymity of the sender when it communicates with other end. A malicious node may try to block the data packets and may try to find destination through traffic analysis by an intersection attack. So the source, destination and route need the protection of anonymity. In communication, a sources sends are quest to a destination D. In PARS, each node uses a dynamic pseudonym as its node identifier rather than using its real MAC address. Anode’s pseudonym expires after a time period in order to prevent attacks. Pseudonym changes in predetermined time intervals. Each node piggy backs its updated position and pseudonym to its neighbors by”hello” messages. All the nodes maintain a routing table that keeps its neighbors pseudonym sand their locations. The destination node position determines the routing.

B. Zone partition

In PARS the communication range is partitioned in to the Zones. The source and destination are not present in the same zone. During the Zone partition the condition to be considered is, the forwarder and the destination not present in the same zone. Till this condition satisfied it will be portioned in to horizontal and vertical zones. In this, Random forwarder is selected randomly in the zone. RF is selected in the following way. First the randomly the location is selected from the particular Zone. The node nearest to the location is elected as the Random Forwarder.

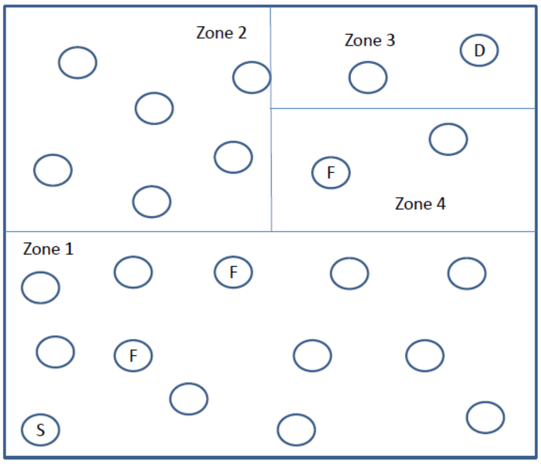

Figure1.Zonepartition

C. Routing scheme

PARS feature a dynamic and unpredictable routing path, which consists of a number of intermediate random forwarders. As shown in figure, horizontally partition the network into two zones A1 and A2 based on the distance between source and destination. PARS uses the hierarchical zone partition and randomly chooses a node in the partitioned zone in each step as an intermediate relay node (i.e., data forwarder), thus dynamically generating an unpredictable routing path for a message.

.

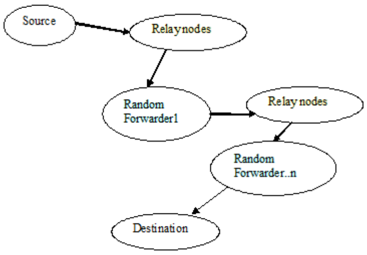

Figure2.Routing Scheme

The destination zone consisting of k nodes and is used to control the degree of anonymity protection for the destination. In the PARS routing, each data source or forwarder executes the hierarchical zone partition. The procedure checks whether the source node and destination are in the same zone. If so, it divides the zone in to two. The process repeated until when it and ZD are not in the same zone. The node randomly chooses a position in the other zone called and uses the GPSR routing algorithm to send the data to the node closest to that position. That node is known as a random forwarder (RF).In routing scheme source node and each forwarder node broadcasts the packet to n neighbors. If the source has not received the confirmation within the time period, it will resend the packets.

D. Anonymity

Increase the anonymity protection of the source light weight mechanism called" broadcast to neighbors" issued. Dead end is problem in the geographic routing in which each node is aware of the positions of its neighbors to forward a packet to the neighbor that is nearest to the destination. Dead end occurs when a packet is forwarded to a node whose neighbors are away from the destination than itself and the packet is routed between neighbors. To avoid dead end problem the PARS can incorporate face routing. The transmission is based on a set of random forwarders they decide which location the packet should be sent to. Between any two RFs, some nodes as relays to perform the GPSR routing. Each node has no information on the S or D except the destination zone information. Routing is based on the coordinate of the next TD.

This proposed protocol offers identity and location anonymity of the source destination and route anonymity. This procedure chooses the shortest path and it makes the route between an S-D pair difficult to observe by randomly and dynamically selecting the intermediate nodes and zone partition. So it is difficult for an intruder to observe a transmission pattern.

The intermediate nodes are only aware of its proceeding and succeeding node in route and the source and destination nodes cannot be differentiated from other nodes route. The anonymous path between S and D guarantees that nodes on the path do not know where the terminal nodes are. PARS also provide n-anonymity to destinations by hiding D among n receivers in ZD. An attacker can get the destination zone position rather than the position of destination.Eachrandomforwarderbroadcastthatpackettoitsallneighbours including the next hop. The route anonymity due to random relay node selection in this scheme prevents an attacker from intercepting packets or to issue DoS attacks. The routes between two communicating nodes are changing that makes difficult for attackers to predict the route of the next packet.

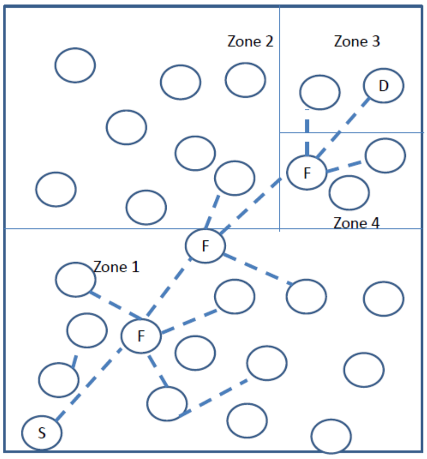

Figure3. Anonymous routing

IV. Performance evaluation

Finally, in the last part we made the similar scenario using GPSR protocol. The presence of malicious nodes does not ensure reliability of data packets. Then, in this module, a comparison between the proposed system and the existing GPSR is made, based on the through put. It is observed that the proposed system gives higher through put Anonymous Position based Routing Scheme provides the anonymity by limiting a node's view only to its neighbors. This makes difficult for an attacker to differentiate a node as whether it is a source or a forwarding node. Next, a comparison between the same was made based on routing overhead. The routing overhead can be measured based on the ratio between routing packets to that of received packets. It is found, nearly similar.

A. Experimental Settings

The performance of PARS is analyzed by using Network Simulator NS-2. Different factors are considered and X graphs are plotted. The performance of the PARS is compared with that of GPSR by considering the following factors like Packet Delivery Ratio, Normalized Overhead and throughput.

The node motion adopted is the random way point. The throughput for both PARS and GPSR is also calculated. Through put is the amount of data delivered per unit time. The throughput larger for the PARS. The X graph for the throughput for both GPSR and PARS is given in figure. Normalized overhead is the overhead that is experienced

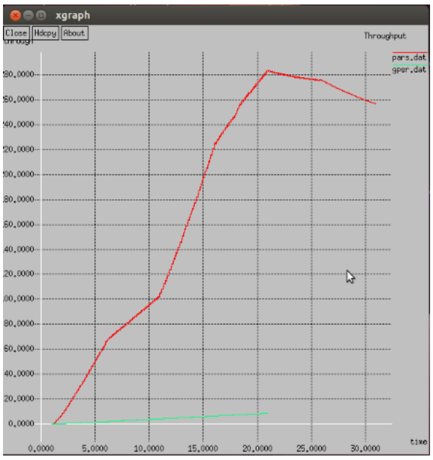

Figure 4. Throughput

While routing a packet. It is also considered for comparing the performance of PARS with that of GPSR. NOH are almost similar to the GPSR scheme. Figure shows the Xgraph based on the comparison of NOH. PDR (Packet Delivery Ratio)

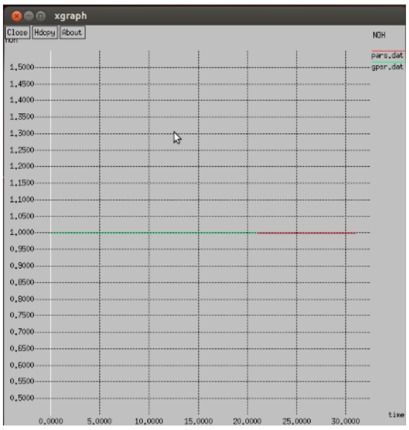

Figure 5.Normalized overhead

is ratio of total amount of packets reached the receiver to the amount of packet sent by source. The PDR decreases with the amount of malicious node increases. The mobility of nodes also result in PDR decrease. PARS uses GPSR based routing. The routing is based on information about immediate neighbours in the network topology. Figure shows the X graph based on the comparison of PDR of PARS and GPSR .The figure shows that the packet delivery ratio of PARS is higher when compared to that of GPSR. The graph shows that the pdr is higher for PARS as compared with GPSR.

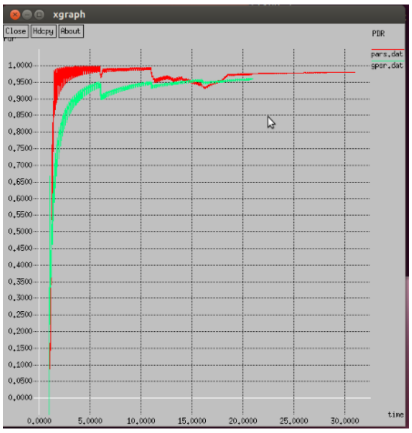

Figure6.Packetdeliveryratio

V. Conclusion and future enhancement

This paper covers the idea about anonymous location- based efficient routing protocol. By anonymous routing protocol are crucial in MANETs to provide secure communications by hiding node identities and preventing traffic analysis attacks from outside attackers. Anonymity in MANETs includes identity and location anonymity of data sources (i.e. Senders) and destinations (i.e. Recipients), as well as route anonymity. Position based Anonymous Routing Scheme (PARS) provides high anonymity protection with low cost. PARS dynamically partition the network field into zones and randomly choose nodes in zones as intermediate forwarder nodes, which form an anonymous route. PARS hide the data source/receiver among many initiators/receivers to strengthen source and destination anonymity protection.

Active research work for MANETs is carrying on mainly in the fields of Medium Access Control, routing schemes, resource management, power control, and security. PARS provide source, destination and route anonymity. Trust is an important concept in network security, defines a relation among entities that participate in various protocols. Trust relations are based on the previous interactions of entities within a protocol. Trust Evaluation of the nodes considered to transfer the data that is trust values of the communicating node considered during the data transfer in the communication, trust values calculated for the each node in the communication. It also improves the security of the system with the privacy .the trust values for each node calculated using there commendation from the other nodes about the node, that trust should be calculated and then, the node want to transfer the data to the other node it considers the trust values of that node, trust values calculated using the recommendation and then the monitoring the performance of the other nodes. So based on these trust values we can identify the malicious nodes. Anonymity means hiding the node identity and route identity. So it is an efficient approach to utilize the dynamic pseudonyms scheme to preserve the nodes' privacy. This tries to use the light weight Hash function to produce pseudonyms which are automatically changed through analyzing received packets.

References

[1]. A. Pfitzmann, M. Hansen, T. Dresden, and U. Kiel,"Anonymity, Unlinkability, Un observability, Pseudonymity, andIdentity Management a Consolidated Proposal for Terminology,Version0.31",technicalreport,2005.

[2]. Z.Zhiand Y.K. Choong,"Anonymizing Geographic AdHoc Routing for Preserving Location Privacy,",Proc.Third Intl Workshop Mobile Distributed Computing (ICDCSW),2005.

[3]. V.Pathak,D.Yao,and L.Iftode,"Securing Location Aware Services over VANETUsing Geographical Secure Path Routing,",Proc.IEEE Intl Conf. Vehicular Electronics and safety (ICVES),2008.

[4]. K.E. Defrawy and G. Tsudik, "ALARM: Anonymous Location- Aided Routing in Suspicious MANETs,",Proc. IEEE Intl Conf. Network Protocols (ICNP), 2007.

[5]. X.Wu,J.Liu,X.Hong, and E.Bertino,"Anonymous Geo- Forwarding in MANETs through Location Cloaking,", IEEE Trans.Parallel and Distributed Systems,vol.19,no.10,pp.1297-1309,Oct.2008.

[6]. K.El-Khatib,L.Korba,R.Song,andG.Yee,"AnonymousSecureRoutinginMobileAd-HocNetworks,",Proc.IntlConf. Parallel Processing Workshops(ICPPW),2003.

[7]. J. Kong, X. Hong, andM. Gerla, "ANODR: Anonymous on Demand Routing Protocol with Untraceable Routes for Mobile AdHoc Networks,", Proc. ACM MobiHoc,pp.291-302,2003.

[8]. H.FreyandI. Stojmenovic On delivery guarantees of face and combined greedy-face routing in ad hoc and sensor networks.",InProc.ofMobiCom,2006.

[9]. X. Hong, M. Gerla, G. Pei, andC.C. Chiang "A group mobility model for adhoc wireless networks.", In Proc. of MSWiM,1999.

[10]. A.R. Beresford and F.Stajano"Mix zones: User privacy in location-aware services.", In Proc.ofPERCOMW,2004.

[11]. HaoYang, Haiyun Luo"Security in mobile adhoc networks: challenges and solutions",WirelessCommunications,IEEE2004.

[12]. Y.-C.Hu,D.B.Johnson,and A.Perrig,SEAD: Secure Efficient Distance Vector Routing for Mobile Wireless Ad Hoc Networks,,Proc.IEEE Workshop Mobile Computing Systems and Applications(WMCSA),2002.

[13]. JinyangLi,JohnJannotti,DouglasS.J.De,CoutoDavid,R.Karger,andRobertMorris"Ascalable locationserviceforgeographicadhocrouting.",InProc.ofMOBICOM,2000.

[14]. KarimElDefrawyandGeneTsudik,"Privacy-PreservingLocation-BasedOn-DemandRouting in MANETs,",IEEE journalonselectedareasincommunicationDecember2011.