ISSN (ONLINE): 2454-9762
ISSN (PRINT): 2454-9762
Available online at www.ijarmate.com

International Journal of Advanced Research in Management, Architecture, Technology and Engineering (IJARMATE) Vol. 2,Special Issue 6, March 2016

SECURED ROUTING FOR MANET'S ADVERSARIAL ENVIRONMENTS

B. Hari Prasad
Asst. Professor
Shree Institute of Technical Education

O. Devakiran
SAN Administrato
EMC, Bangalore

M. Srinivasulu
Asst. Professor
Shree Institute of Technical Education

ABSTRACt: The Mobile Adhoc Networks (MANETs) is remote and element topology system medium, which might experience the ill effects of numerous open security feedback. The real issue of The Mobile Adhoc Networks (MANETs) is to send the information in secure way from source to destination hub in antagonistic (adversary) environment such remote hub correspondence issues are hub activity, hub assault and information getting to of middle hubs. The fundamental point of system is to give unidentifiability and unlinkability to versatile hubs. The current conventions are helpless against the assaults of fake directing packets or Denial-of-Service (DoS) TV, even the hub personalities are ensured by aliases. In this proposed framework another directing convention, i.e., authenticated anonymous secure routing (AASR), to fulfill the necessity and safeguard the assaults has been utilized. All the more particularly, the route ask for packets are validated by a gathering mark, to shield the potential dynamic assaults without revealing the hub personalities. in this paper, we will enhance AASR to diminish the packet delay. The hubs in the same system must help and trust one another in sending packets starting with one hub then onto the next. Notwithstanding, this suggested trust relationship can be undermined by malevolent hubs that might alter or disturb the efficient trade of packets.

Keywords— AASR Protocol, Group Signature, Onion Routing, Mobile Ad Hoc Networks, Secure Routing Protocol (SRP), Trust based Quality of Service (TQoS), Anonymous Routing

I. INTRODUCTION

Mobile ad hoc networks (MANETs) are powerless against security dangers because of the innate attributes of such systems, for example, the open remote medium and element topology. It is hard to give trusted and secure interchanges in ill-adversarial environments, for example, combat zones. On one hand, the foes outside a system might surmise the data about the imparting hubs or movement streams by detached activity perception, regardless of the fact that the interchanges are scrambled. Then again, the hubs inside the system can't be constantly trusted, following a legitimate hub might be caught by adversaries and gets to be vindictive. Therefore, anonymous correspondences are essential for MANETs in antagonistic situations, in which the hubs recognizable pieces of proof and routes are supplanted by irregular numbers or pseudonyms for secure purpose..

Anonymity is characterized as the condition of being unidentifiable inside of an arrangement of subjects. In MANETs, the prerequisites of anonymous communications can be portrayed as a mix of unindentifiability and unlinkability [1]. Unindentifiability implies that the personalities of the source and destination can't be uncovered to different hubs. Unlinkability implies that the route and activity streams between the source and destination hubs can't be perceived or the two hubs can't be connected. The way to executing the mysterious correspondences is to create suitable anonymous secure directing conventions. There are numerous mysterious directing conventions proposed in the previous decade. Our center is the kind of topology-

ISSN (ONLINE): 2454-9762
ISSN (PRINT): 2454-9762
Available online at www.ijarmate.com
International Journal of Advanced Research in Management, Architecture, Technology and Engineering (IJARMATE) Vol. 2,Special Issue 6, March 2016

taking into account request mysterious routing protocols, which are general for MANETs in ill-disposed situations. To add to the mysterious conventions, an immediate strategy is to anonymize the normally utilized on-interest specially appointed directing conventions, for example, AODV [2] and DSR [3]. For this reason, the anonymous security affiliations must be built up among the source, destination, and each middle hub along a route.

The subsequent conventions incorporate ANODR [4], [5], SDAR [6], AnonDSR [7], Cover [8], [9], and Rebate ANODR [10]. In the wake of looking at these conventions, we find that the goals of unindentifiability and unlinkability are not completely fulfilled. For instance, ANODR concentrates on securing the hub or route characters amid a route disclosure process, particularly on the directing packets, e.g., Route Ask for (RREQ) and Route Answer (RREP). ANODR receives a worldwide trapdoor message in RREQ, rather than utilizing the ID of the destination hub. Nonetheless, the route can be recognized by an unveiled trapdoor message, which might be discharged to the middle hubs in reverse RREP sending. Alternate conventions depend on the area identification and validation, yet might mostly abuse the namelessness necessities for execution contemplations. For instance, in SDAR, the hub and its onehop neighbors are made to know one another's ID amid the directing methods. In AnonDSR, the halfway hubs on the way might be uncovered to the destination hub. In Cover and Rebate ANODR, an unmistakable hub ID is utilized as a part of the route revelation.

These conventions are additionally helpless against the dissent of-administration (DoS) assaults, for example, RREQ based television. Because of the absence of packet validation, it is troublesome for the conventions to check whether a packet has been adjusted by a malignant hub. As of late, gathering mark is acquainted with anonymous directing. In A3RP [11], the steering and information packets are secured by a gathering mark. Be that as it may, the anonymous route is ascertained by a protected hash capacity, which is not as versatile as the scrambled onion component. In this work, we concentrate on the MANETs in ill-disposed situations, where the general population and gathering key can be at first sent in the portable hubs. We expect that there is no online security or restriction administration accessible when the system is conveyed. We propose a confirmed mysterious secure directing (AASR) to conquer the pre-said issues. We receive a key-scrambled onion to record a found route and plan an encoded mystery message to check the RREQ-RREP linkage. Bunch mark is utilized to verify the RREQ packet per jump, to keep middle of the road hubs from changing the directing packet. Broad recreations are utilized to contrast the execution of AASR with that of ANODR, an agent on-interest mysterious directing convention. The outcomes demonstrate that, it gives more throughput than ANODR under the packet dropping assaults, in spite of the fact that AASR encounters more cryptographic operation delay.

II. LITERATURE SURVEY

In this section, we introduce the basic concepts in anonymous routing, and provide a short survey on the existing routing protocols.

A. Anonymity and Security Primitives We introduce some common mechanisms that are widely used in anonymous secure routing.

1) Trapdoor: In cryptographic functions, a trapdoor is a typical idea that characterizes a restricted capacity between two sets [12]. A worldwide trapdoor is a data gathering component in which middle of the road hubs might include data components, for example, hub IDs, into the trapdoor. Just certain hubs, for example, the source and destination hubs can open and recover the components utilizing pre-set up mystery keys.The utilization of trapdoor requires a mysterious end-to-end key understanding between the source and destination.

2) Onion Routing: It is a component to give private correspondences over an open system [13]. The source hub sets up the center of an

ISSN (ONLINE): 2454-9762
ISSN (PRINT): 2454-9762
Available online at www.ijarmate.com
International Journal of Advanced Research in Management, Architecture, Technology and Engineering (IJARMATE) Vol. 2,Special Issue 6, March 2016

onion with a particular route message. Amid a route ask for stage, every sending hub adds an encoded layer to the route ask for message. The source and destination hubs don't inexorably know the ID of a sending hub. The destination hub gets the onion and conveys it along the route back to the source. The middle of the road hub can confirm its part by decoding and erasing the external layer of the onion. In the end a mysterious route can be set up.

3) Group Signature: Group signature plan [14] can give validations without exasperating the namelessness. Each part in a gathering might have a couple of gathering open and private keys issued by the gathering trust power (i.e., bunch chief). The part can produce its own particular mark by its own private key, and such mark can be checked by different individuals in the gathering without uncovering the underwriter's character. Just the gathering trust power can follow the endorser's character and disavow the gathering keys.

B. Anonymous On-demand Routing Protocols

There are numerous mysterious on-interest routing protocols. Like the impromptu directing, there are two classifications: topology-based and area based [1], or at the end of the day, hub character driven and area driven [15]. We look at the conventions in Table I, as far as the key conveyance suspicion, hub obscurity in route disclosure, and packet confirmation. Our perceptions are abridged as takes after: As a matter of first importance, the directing conventions are intended to work in various situations. AO2P, Crystal, and Alarm are intended for area based or area helped anonymous correspondences, which require confinement administrations. Since our own is for general MANETs, we concentrate on the topology-based directing instead of area based steering. Furthermore, as said in Segment I, SDAR, AnonDSR, Veil, and D-ANODR have issues in meeting the unindentifiability and unlinkability. The hub IDs in an area and along a route are conceivably uncovered in SDAR and AnonDSR, individually. The plain hub IDs are utilized as a part of the route demand of Cover and D-ANODR. In this work, we utilize the hub's pen name of its genuine ID, to maintain a strategic distance from the data spillage amid RREQ and RREP forms. Thirdly, a percentage of the conventions receive extra validation plans to sign the steering packets, including A3RP, RAODR [17], USOR [18], and Crystal [20]. Note that, despite the fact that Veil gives neighborhood confirmation, it can't sign the directing packets. RAODR conveys an expert key component, which can't give the obscurity, traceability, and enforceability that are bolstered by a gathering mark. A3RP and USOR receive a gathering mark and utilize secure hash capacities to outline keys and hub nom de plumes a route. We pick the onion based steering to record the anonymous routes, in light of the fact that the onion is more versatile than different components and can be stretched out, for instance to various ways. Fourthly, we have to reexamine the suspicions on the key dispersion and hub obscurity in route disclosure. For instance, ARM accept that the source and destination hubs share a long haul session key ahead of time, which is not viable for genuine MANETs. We expect that the hubs are outfitted with open and private keys amid system instatement stage and can create the common symmetric key in an ondemand way.

III. NETWORK CASES

A. Adversaries and Attack Models Without loss of all inclusive statement, we accept that an enemy knows all the system conventions and capacities. The assailants outside the system don't have the foggiest idea about the mystery keys, however those inside the system might know the keys. We characterize their assaults as per their practices (e.g., dynamic or inactive) and areas (e.g., inside or outside the system). Uninvolved outside assault: There might be an outer worldwide latent foe, who can watch and record all the remote interchanges in the system. It will attempt to uncover the characters of the source, destination, and on the way hubs of a specific stream, or gather the movement streams by connecting the packets to the source or destination hubs. Dynamic outside assault: The aloof aggressors maintain a strategic distance

ISSN (ONLINE): 2454-9762
ISSN (PRINT): 2454-9762
Available online at www.ijarmate.com
International Journal of Advanced Research in Management, Architecture, Technology and Engineering (IJARMATE) Vol. 2,Special Issue 6, March 2016

from any assault that uncovers their activities since they endeavor to be imperceptible, yet the dynamic outside assailants don't have such confinements. They might intend to upset the directing or dispatch a DoS assault. They can move from here to there and dispatch assaults arbitrarily. Latent inside assault: The assailants are honest to goodness MANET hubs. Like the inactive outside assailants, they will attempt to deduce the personalities of the source, destination, or enroute hubs without uncovering themselves. Since they can read the genuine packets, the movement example or hub portability data might be learned by them. Dynamic inside assault: They can alter, infuse, and replay real messages. They can likewise take on the appearance of different hubs and dispatch the mimic assaults. They can make one or more ghost hubs by producing legitimate steering packets.

B. Network Assumptions We denote a MANET by **T** and make the following assumptions.

1) Public Key Infrastructure: Each node **T** initially has a pair of public/private keys issued by a public key infrastructure (PKI) or other certificate authority (CA). For node *A* (*A* □ **T**), its public/private keys are enoted by *KA*+ and *KA*□. Similar to the existing secure routing [22], we assume that there exists a dynamic key management scheme in **T**, which enables the network to run without online PKI or CA services.

2) Group Signature: We consider the entire network **T** as a group and each node has a pair of group public/private keys issued by the group manager. The group public key, denoted by *GT*+, is the same for all the nodes in **T**, while the group private key, denoted by *GA*- (for *A* □ **T**), is different for each node. Node *A* may sign a message with its private key *GA*-,and this message can be decrypted via the public key *GT*+ by the other nodes in **T**, which keeps the anonymity of *A* [14]. We also assume that there exists a dynamic key management scheme working together with the admission control function of the network, which enables the group signature mechanism running properly. Such assumptions are also adopted in the existing work of military ad hoc networks [17], [23].

3) Neighborhood Symmetric Key: Any two hubs in an area can set up a security affiliation and make a symmetric key with their open/private keys. This affiliation can be activated either by a periodical Hi messages or by the directing revelation RREQ messages. For two hubs An and B (A;B ∈ T), the common symmetric key is meant by KAB and utilized for the information transmissions between them. There are some methodologies supporting the foundation of one-jump shared key, for example, Veil, RAODR, and USOR. In this work, we expect one of the methodologies is accessible in T.

IV. PROPOSED WORK

Anonymous communications are imperative for MANETs in ill-disposed situations, in which the hubs recognizable pieces of proof and routes are supplanted by irregular numbers or nom de plumes assurance reason. In a proposed plan, we utilize a Verified Mysterious Secure Directing Convention. The ondemand impromptu steering as the base of our convention, including the periods of route disclosure, information transmission, and route support . After completion the route finds the source hub scramble the message and send to the destination hub this information transmission is secure between source to destination. This module discover the right destination in view of security reason, It exchange the information after the protected route to be established.

Anonymous Onion Routing:

Once the anonymous association is built up, it can convey information. Before sending information over an anonymous association, the onion intermediary includes a layer of encryption for every onion switch in the route. As information travel through the anonymous association, every onion switch evacuates one layer of encryption, so it lands at the responder as plaintext. This layering happens in the opposite request for information moving back to the initiator. In this manner information that

ISSN (ONLINE): 2454-9762
ISSN (PRINT): 2454-9762
Available online at www.ijarmate.com
International Journal of Advanced Research in Management, Architecture, Technology and Engineering (IJARMATE) Vol. 2,Special Issue 6, March 2016

have gone in reverse through the mysterious association must be over and again present crypted on acquire the plaintext. strong bend.

Routing Procedure

The routing algorithm can be implemented based on the existing on-demand ad hoc routing protocol like AODV or DSR. The main routing procedures can be summarized as follows:

1) During route discovery, a source node broadcasts an RREQ packet in the format of (1).
2) If an intermediate node receives the RREQ packet, it verifies the RREQ by using its group public key, and adds one layer on top of the key-encrypted onion, as (7). This process is repeated until the RREQ packet reaches the destination or expired.
3) Once the RREQ is received and verified by the destination node, the destination node assembles an RREP packet in the format of (9), and broadcasts it back to the source node.
4) On the reverse path back to the source, each intermediate node validates the RREP packet of (2) and updates its routing and forwarding tables. Then it removes one layer on the top of the key-encrypted onion, and continues broadcasting the updated RREP in the format of (10).
5) When the source node receives the RREP packet, it verifies the packet, and updates its routing and forwarding tables. The route discovery phase is completed.
6) The source node starts data transmissions in the established route in the format of (11). Every intermediate node forwards the data packets by using the route pseudonym.

V. PROTOCOL DESIGN

In this section, we show the configuration of AASR convention. Considering the nodal versatility, we take the on-interest specially appointed directing as the base of our convention, including the periods of route revelation, information transmission, and route upkeep. In the route revelation stage, the source hub shows a RREQ packet to each hub in the system. On the off chance that the destination hub gets the RREQ to itself, it will answer a RREP packet back along the approaching way of the RREQ. Keeping in mind the end goal to ensure the obscurity while trading the route data, we upgrade the packet arrangements of the RREQ and RREP, and adjust the related procedures. As a case, we utilize a five-hub system to represent the verified unknown directing procedures. The system is appeared in Fig.1, in which the source hub S finds a route to the destination hub D.

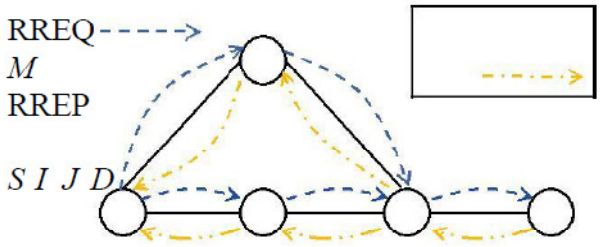


Fig. 1. Network topology

privacy information about the two communication parties that discover the route.

1) *Identity Anonymity:* Our routing protocol can work without utilizing the hubs' characters. Every one of the hubs create arbitrary nonce to show themselves. Thus, any halfway or foe hubs can't procure the personalities of the source and destination hubs. Other than the trapdoor data dest in the RREQ packet, there is no identityrelated data included in steering and sending forms. Notwithstanding, in ANODR, dest is additionally utilized as a part of the RREPs in reverse sending. A halfway malevolent hub can utilize it to gather the destination. In AASR, we receive an encoded mystery VSD as the check message in the RREP stage. Despite the fact that Nv and Kv will be known by the middle of the road hubs in route disclosure, they are not identified with the destination's character. Along these lines, AASR gives preferable unindentifiability and unlinkability over ANODR.

2) Route Anonymity: Amid the route disclosure, the Source, moderate, and destination hubs just have data about the hubs' pen names the past and next jump. Regardless of the fact that a hub takes an interest in route disclosure, it has no

ISSN (ONLINE): 2454-9762
ISSN (PRINT): 2454-9762
Available online at www.ijarmate.com
International Journal of Advanced Research in Management, Architecture, Technology and Engineering (IJARMATE) Vol. 2,Special Issue 6, March 2016

clue about the whole route, neither an outside enemy.

Following the nonce of destination hub is one-time arbitrarily produced and just known by its neighborhood, it is hard for the agreeable and malignant hubs to induce the multi-bounce route.

3) Location Anonymity: The packet arrangement of AASR does exclude any data identified with the system topology and the quantity of partaking hubs, (for example, TTL and grouping). In this way within vindictive hub can't construe the system topology. One potential issue of our convention is that the measure of the key-scrambled onion might increment with the quantity of jumps along the RREQs television way. By expecting a most extreme number of jumps, and settled message size, and irregular TTL strategy [11], [16], such issue can be determined. Because of as far as possible, we don't display the subtle elements here. With the arrangement of the procedure, the outside malignant hub can't deduce the jump number by watching the packet size. no thought regarding the whole route, neither an outside enemy. Following the nonce of destination hub is one-time haphazardly produced and just known by its neighborhood, it is hard for the agreeable and pernicious hubs to gather the multi-bounce route.

Security Analysis

Passive Attacks: One sort of passive attacks is a worldwide spy. As talked about in the past segment, it is unimaginable for a spy to acquire the character data about the source or adestination hub in any correspondence session in AASR. Another sort of latent assault is the quiet dropping, which implies the enemies or childish hubs noiselessly decline to perform the asked for capacities in the convention. In ordinary steering conventions, the guard dog model can be utilized to identify such activities. Be that as it may, in the unknown versatile correspondence, it is difficult to perceive the mischief of enemies or narrow minded hubs. In AASR, this can be enhanced by presenting a hub trust model [24].

Impersonation Attacks: Impersonation attacks can be launched by the inside attackers. For example, the RREQ packets may be read and modified in some anonymous routing protocols. While in AASR, any node without the group key cannot join the communications. Because the forgery of a group signature is computational infeasible, it is impossible for an adversary to modify the packets. Since the group signature is traceable, if a group manager is available in the network, the singer of the fake routing packet can be identified by the group manager with the group's master key.

DoS Attacks: DoS attacks aim to deplete the nodes' resources. If the attacks are launched by the outside adversaries not having the keys, the packets can pass the packet verification. Such DoS attacks have little threat on our protocol. If the attacks are launched by the inside adversaries, more damage will be caused. However, once an inside adversary does so, its behavior of sending a large amount of route requests can be detected by other nodes in its neighborhood. Such abnormal behavior will be reported to the group manager. Then the attacker will be identified by tracing its signature.

Performance Simulation

We implement the projected AASR protocol in ns-2(2.34) by extending the AODV module to support the scientific discipline operations. We tend to compare the performances of AASR of existing and with trust algorithmic rule to those someone situations.

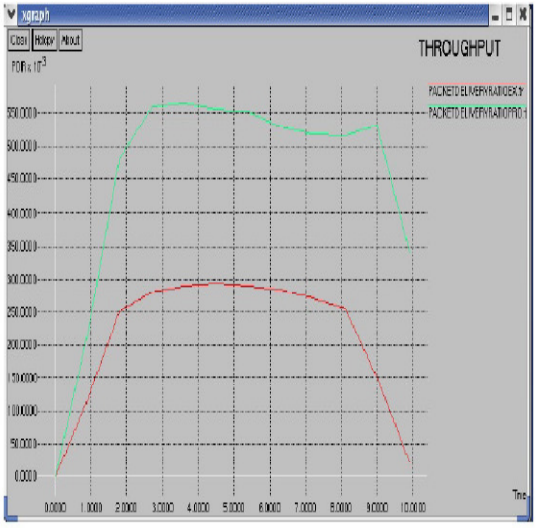
Performance Evaluation Metrics

To evaluate the performance of routing protocols quantitative metrics square measure practiced. The six vital performance metrics square measure for analysis of routing protocols is as follows:

1. Throughput - turnout is that the live of how briskly we are able to really send packets through network. The amount of packets delivered to the receiver provides the turnout of the network. The turnout is outlined because the total quantity of knowledge a receiver really receives from the sender divided by the time it takes for receiver to urge the last packet. In our

ISSN (ONLINE): 2454-9762
ISSN (PRINT): 2454-9762
Available online at www.ijarmate.com
International Journal of Advanced Research in Management, Architecture, Technology and Engineering (IJARMATE) Vol. 2,Special Issue 6, March 2016

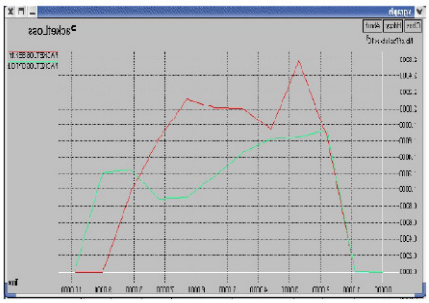
proposed system throughput is increases 45% with respect to existing system.



a. Throughput

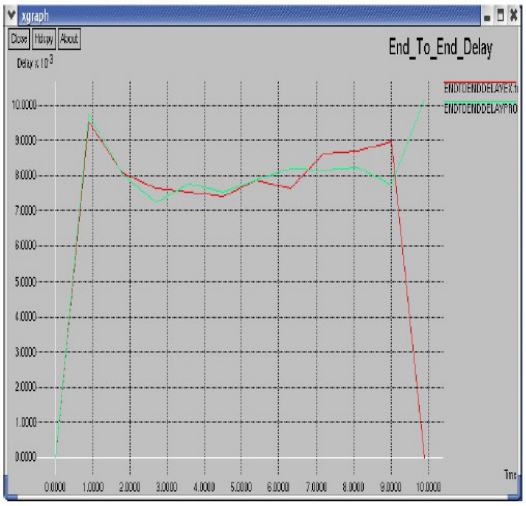
2. Packets born - a number of the packets generated by the supply can get born within the network thanks to high quality of the nodes, congestion of the network etc. In our proposed system packet loss is reduced by 13.88% with respect to existing system.

3. Packet Delivery Ratio - The magnitude relation of the information packets delivered to the destinations to those generated by the CBR sources. It's the fraction of packets sent by the applying that square measure received by the receivers.



b. Pack loss ratio

5. End-to-End Delay – End-to-End delay indicates however long it took for a packet to travel from the supply to the applying layer of the destination, .i.e. the full time taken by every packet to achieve the destination. Average End-to-End delay of knowledge packets includes all potential delays caused by buffering throughout route discovery, queuing delay at the interface, retransmission delays at the mack, propagation and transfer times. In our proposed system end-to-end delay have the 0.82% that is relatively decreasing with existing system



c. End-to-End Delay

5. Optimal Path Length - it's the magnitude relation of total forwarding time to the overall range of received packets. Optimum path length will increase as range of hops on optimum path will increase.

VI. CONCLUSION

In this paper, we outline a authenticated and anonymous routing protocol and for MANETs in ill-disposed situations. The route ask for bundles are validated by gathering marks, which can safeguard the potential dynamic anonymous assaults without uncovering the hub personalities. By consolidating the security instrument with QoS necessities, we display a safe QoS routing protocol that accomplishes better execution. In this paper, we proposes

ISSN (ONLINE): 2454-9762
ISSN (PRINT): 2454-9762
Available online at www.ijarmate.com
International Journal of Advanced Research in Management, Architecture, Technology and Engineering (IJARMATE) Vol. 2,Special Issue 6, March 2016

Trust based Nature of Administration (TQoS) gives secure correspondence and to lessen the parcel misfortune proportion. The key-encoded onion steering with a course mystery confirmation message is intended to record the unknown courses as well as keep the middle of the road hubs from construing the genuine destination. The Connection State Model is accustomed to recognizing the connection disappointments in the foe environment. In our future work, we will utilize improved AASR convention to decrease activity. A conceivable strategies is to consolidate Caution [3] convention used to dispense with the vindictive hub in the adversary environment.

REFERENCES

[1] D. Boneh, X. Boyen, and H. Shacham, "Short group signatures," in Proc. Int. Cryptology Conf. (CRYPTO'04), Aug. 2004.

[2] S. William and W. Stallings, Cryptography and Network Security, 4thEdition. Pearson Education India, 2006.

[3] K. E. Defrawy and G. Tsudik, "ALARM: Anonymous Location-Aided Routing in Suspicious MANETs," IEEE Trans. on Mobile Computing, vol. 10, no. 9, pp. 1345–1358, Sept. 2011.

[4] Y. Zhang, W. Liu, W. Lou, and Y. G. Fang, "MASK: Anonymous On-Demand Routing in Mobile Ad hoc Networks," IEEE Trans. on Wireless Comms., vol. 5, no. 9, pp. 2376–2386, Sept. 2006.

[5] M. Yu and K. Leung, "A Trustworthiness-based QoS routing protocol for ad hoc networks," IEEE Trans. on Wireless Comms., vol. 8, no. 4, pp. 1888–1898, Apr. 2009.

[6] D. Boneh and M. Franklin, "Identify-based encryption from the weilpairing," inProc. CRYPTO'01, ser. LNCS, vol. 2139. Springer-Verlag, 2001, pp. 213–229.

[7] P. Barreto, H. Kim, B. Bynn, and M. Scott, "Efficient algorithms for pairing-based cryptosystems," inProc. CRYPTO'02,ser. LNCS, vol. 2442. Springer-Verlag, 2002, pp. 354–368.

[8] M. G. Reed, P. F. Syverson, and D. M. Goldschlag, "AnonymousConnections and Onion Routing," IEEE Journal on Selcted Area in Comm., vol. 16, no. 4, pp. 482–494, May 1998.

[9] K. E. Defrawy and G. Tsudik, "Privacy-Preserving Location-Base d On-Demand Routing in MANETs," IEEE Journal on Selected Areas in Communications, vol. 29, no. 10, pp. 1926–1934, Dec. 2011.

[10] J. Kong and X. Hong. ANODR: ANonymous On Demand Routing with untraceable routes for mobile ad-hoc networks. InACM MOBIHOC'03, 2003.

[11] Wei Liu and Ming Yu, "AASR: Authenticated Anonymous Secure Routing for MANETs in Adversarial Environments" IEEE transactions on vehicular technology, vol. x, no. y, march 2014. [12] M. Yu, M. C. Zhou, and W. Su, "A secure routing protocol against Byzantine attacks for MANETs in adversarial environment," IEEE Trans.on Vehicular Tech., vol. 58, no. 1, pp. 449–460, Jan. 2009.

[12] Mr. P. Dhakshinamoorthi and Dr. M. Balachandran "Trust Nodes Routing Technique for Manet in Adversarial Environments" IJAICT Volume 1, Issue 6, October 2014.

[13] Wei Liu and Ming Yu "AASR: Authenticated Anonymous Secure Routing for MANETs in Adversarial Environments" IEEE Transactions On Vehicular Technology, Vol. X, No. Y,March 2014.

[14] JojySaramma John, R.Rajesh "Efficient Anonymous Routing Protocols in Manets" International Journal of Computer Trends and Technology (IJCTT) – volume 11 number 1 – May 2014.

[15] R. Menaka, Dr. V. Ranganathan " A Survey of Trust related Routing Protocols for Mobile Ad Hoc Networks" International Journal of Emerging

ISSN (ONLINE): 2454-9762
ISSN (PRINT): 2454-9762
Available online at www.ijarmate.com
International Journal of Advanced Research in Management, Architecture, Technology and Engineering (IJARMATE) Vol. 2,Special Issue 6, March 2016

Technology and Advanced Engineering Volume 3, Issue 4, April 2013.

[16] M. Gunasekaran and K. Premalatha " POR: Privacy- Preserving On-Demand Routing Scheme to Mitigate Malicious Nodes in Mobile Ad Hoc Networks" International Journal of Computer Applications Volume 82, November 2013.

[17] Merin Francis , M. Sangeetha and Dr. A. Sabari " Key Management Technique for Secure and Reliable Data Transmission in MANET" International Journal of Advanced Research in Computer Science and Software Engineering Volume 3, Issue 1, January 2013.

[18] Patil V.P " Efficient AODV Routing Protocol for MANET with enhanced packet delivery ratio and minimized end to end delay" International Journal of Scientific and Research Publications, Volume 2, Issue 8, August 2012.

[19] DurgeshWadbudeand VineetRichariya" An Efficient Secure AODV Routing Protocol in MANET" International Journal of Engineering and Innovative Technology (IJEIT) Volume 1, Issue 4, April 2012.

[20] PriyankaGoyal ,VintiParmar , Rahul Rishi "MANET: Vulnerabilities, Challenges, Attacks, Application" IJCEM International Journal of Computational Engineering & Management, Vol. 11, January 2011

[21] PushpitaChatterjee "Trust Based Clustering And Secure Routing Scheme For Mobile Ad Hoc Networks" International Journal of Computer Networks & Communications (IJCNC), Vol.1, No.2, July 2009.

[22] S. William and W. Stallings, Cryptography and Network Security, 4th Edition. Pearson Education India, 2006.

[23] Jiejun Kong and Xiaoyan Hong "ANODR: Anonymous On Demand Routing with Untraceable Routes for Mobile Adhoc Networks" MobiHoc'03, Jun. 2003, pp. 291–302.

[24] Y. Zhang, W. Liu, and W. Lou, "Anonymous communications in mobile ad hoc networks," in Proc. IEEE INFOCOM 2005, vol. 3, Mar. 2005, pp. 1940–1951.

[25] M. G. Reed, P. F. Syverson, and D. M. Goldschlag, "Anonymous Connections and Onion Routing," IEEE Journal on Selcted Area in Comm., vol. 16, no. 4, pp. 482–494, May 1998.

[26] Network Simulator Documentation at http://www.isi.edu/nsnam/ns/

[27] Network Simulator Installment http://sourceforge.net/projects/nsnam/files/allinone/nsallinone-2.35/

[28] www.wikipedia.com

[29] R. Song and L. Korba, "A robust anonymous ad hoc ondemand routing," in Proc. IEEE MILCOM'09, Oct. 2009.

[30] M. Yu, M. C. Zhou, and W. Su, "A secure routing protocol againstByzantine attacks for MANETs in adversarial environment," IEEE Trans.on Vehicular Tech., vol. 58, no. 1, pp. 449–460, Jan. 2009.

[31] X. Hong, J. Kong, Q. Zheng, N. Hu, and P. Bradford, "A HierarchicalAnonymous Routing Scheme for Mobile Ad-Hoc Networks," in Proc.IEEE MILCOM'06, Oct. 2006.

[32] X.Wu and B.Bhargava, " AO2P:Ad Hoc On-Demand Position-BasedPrivate Routing Protocol, " IEEE Trans. On Mobile Computing, vol. 4,no. 4, pp. 335-348, July/Aug.2005