ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

*(An ISO 3297: 2007 Certified Organization)*

**Vol. 4, Issue 6, June 2016**

# A Survey on Anonymous Routing Protocols in MANETs

A. Naveena[1], Dr. K. Ramalinga Reddy[2]

Assistant Professor, Dept. of ETM., G. Narayanamma Institute of Technology and Science, Hyderabad, India

Professor, HOD, Dept. of ETM, G. Narayanamma Institute of Technology and Science, Hyderabad, India

**ABSTRACT**: Mobile ad hoc network(MANET) represents a complex distributed system that consists of wireless mobile nodes , that can be self organised into different network topologies. Due to complex nature of MANETs and resource constraints nodes , there has been always the requirement of security and privacy in MANET.A number of routing protocols have been proposed to maintain the security and privacy but they are compromised because of the absences of centralised architecture. To avoid the communication between the nodes being compromised, Anonymity is introduced in communication. The concept of Anonymity is that, the communication among the nodes is done without revealing the real identity of nodes to its neighbour or to third party. This paper proposes the survey of the Anonymity based routing protocols with its limitations.

**KEYWORDS**: Anonymous, routing, privacy, security, MANET

## I. INTRODUCTION

Mobile Ad Hoc Networks (MANETs) is the collection of mobile nodes which are not restricted in any infrastructure. These nodes can communicate with each other and can roam anywhere without limitations. The feature of unrestricted mobility makes MANET highly suitable for emergencies, natural disaster and military operations.

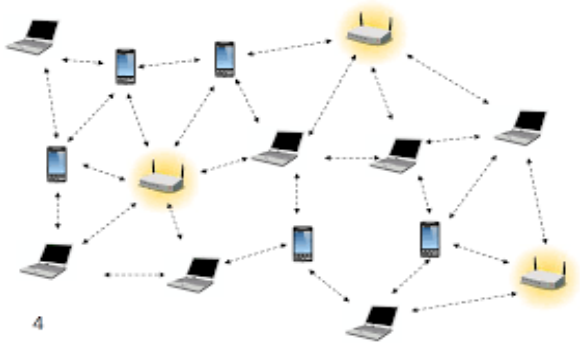

Fig 1. Mobile adhoc Network

Due to the lack of centralized infrastructure and resource constrained nodes , the communication among the nodes is vulnerable to different security attacks. To maintain the privacy and security in communication, Anonymity is introduced in identity ,location and in route. First, Anonymity in identity stands for hiding the real identity of nodes in front of neighbours and third party. Second, Anonymity in location stands for hiding the exact location of source and destination except themselves. Third, Anonymity in route means to avoid the tracing of the route of transmission of packets by attacker.

Complete Anonymity comprises of three important terms. Those are Unlinkability,Unobservability,Pseudonymity. Content Unlinkability means that the content of a message is not linkable and user unlinkability means that it is untraceable who communicates with whom. Similarly, the content unobservability means that useful information can't be extracted from any content and traffic pattern unobservability means that useful information can't be obtained from traffic analysis. Last, pseudonimity means to provide anonymity for the sender and receiver identity.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

*(An ISO 3297: 2007 Certified Organization)*

**Vol. 4, Issue 6, June 2016**

Several anonymity based routing protocols has been proposed to maintain privacy and security in communication. Again, the routing protocols may be proactive or reactive. Here is the survey of papers based on anonymous routing protocol which are proactive or reactive.

## II. LITERATURE SURVEY

**1. ANODR: Anonymous On Demand Routing with Untraceable Routes for Mobile Adhoc Networks:**

The proposed ANODR [3] is deployed in hostile environment to protect it from inference and intrusion. Untraceable routes or packet flows are created in an on-demand routing environment by using route pseudonym. To achieve anonymity and unlinkability, ANODR uses one-time public/private key pairs .

ANODR have the routing process as anonymous route discovery , anonymous data forwarding.

**1.Anonymous route discovery**: This is a critical procedure which establishes random route pseudonyms for an on demand route. A source broadcasts RREQ packet locally to initiate this discovery procedure. Each packet contains a global unique sequence number , a trapdoor that can be open by destination and an onion. This cryptographic onion is of 3 types i.e. public key protected onion (PO) where the forwarding node encrypts the result with its own public key, ANODR-BO where forwarding node encrypts the result with its symmetric key, ANODR-TBO where the forwarding node joins a random nonce to the boomerang onion.

**2. Anonymous data forwarding**: In this process, the source wraps its data packets by using the route pseudonyms in its forwarding table and then broadcasts them locally without identifying the sender and the local receiver identity.

The advantages of this protocol are that

1. ANODR uses one time public and private key to achieve anonymity in MANET.
2. ANODR prevents the strong attacks, such as node intrusion and omnipresent eavesdropping.

The disadvantages of this scheme is that

1. The ANDOR fails to achieve content unobservability.

**2.An efficient secure distributed anonymous routing protocol for mobile and wireless ad hoc networks**

The main objectives of the proposed protocol SDAR [8] are to provide security, reliability and to allow trust worthy intermediate node to participate in data transmission process. This protocol is suitable for hostile environment, where secure data transmission is the prerequisite.

Contrary to other protocols, this protocol doesn't involve the source in the process of gathering the information about topology. Instead, the source sends the path discovery process to its neighbouring nodes to create an anonymous route. The trust management approach is being followed in this protocol where the trust level is calculated from the past behaviour of the node. Upon receiving the path discovery message, the trust worthy intermediate nodes encrypt the message by community keys and then append their IDs and session keys to the message to resend it to the selected neighbour. Next, the receiving node receives the information about the intermediate nodes by decrypting the message with its private key. Then, encapsulation of this information is done in a multi-layered message by receiver to send it along a reverse path. In the reverse path, each intermediate nodes decrypt the layers one after another and forwards to its predecessor node. This process continues unless it reaches the source node. In this way, the source node gets the information about all intermediate nodes.

The advantages of this protocol are that,

1.This protocol doesn't require the global view of network topology, as it is a non source based routing protocol.
2.This protocol provides resilience towards path hijacking which means the intended receivers only can send the path discovery message which is being accepted by source.

The disadvantages of this scheme are that,

1.It can't deal with trapdoor issues.
2.This protocol doesn't provide mechanism to withstand DoS attack.

**3.MASK: Anonymous On-Demand Routing in Mobile Ad Hoc Networks:**

To maintain Anonymity in MAC layer as well as network layer, the proposed MASK [2] protocol offers anonymity in identity of sender and receiver as well as in their relationship. This MASK protocol also assures

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

*(An ISO 3297: 2007 Certified Organization)*

**Vol. 4, Issue 6, June 2016**

unlocatability, untrackability and end to end flow untracebility. Dynamic pseudonyms are used rather than static MAC and network addresses ,to maintain anonymity in MAC layer.

The following steps are involved in this protocol: Anonymous MAC layer communication, ,Anonymous network layer communication.

**1.Anonymous MAC layer communication**: First of all, a trusted authority (TA) gives the pairing parameters along with a group-wise master key to the members of the MANET. Then dynamic pseudonyms are substituted in place real IDs with secrete point set by the nodes . Anonymous authentication in MAC layer sets up a secret handshaking between two neighbouring nodes of the same group to identify each other. The node establishes shared master key and link identifier with all of its neighbouring nodes to maintain anonymity .In order to avoid hidden and expose terminal problem the conventional RTS-CTS-DATA-ACK frame exchange scheme is used.

**2.Anonymous network layer communication:** A multipath route is established between source and destination with multiple hops. Each node maintains routing tables which are forwarding routing table, reverse routing table and target linkID routing table. First, each node broadcasts anonymous route request .It contains global unique identifier, last sequence number of destination, active pseudonym of source . Upon receiving ARREQ message for the first time, the intermediate node inserts an entry into its reverse routing table and then rebroadcasts the ARREQ after placing the embedded pseudonym in routing table. This process continues until all the nodes in the network have rebroadcasted the ARREQ once. An anonymous route reply (ARREP) is generated and sent back to the source at the destination or at any intermediate node which has a valid route to the destination.

The advantages of this are that,

1.MASK achieves high routing efficiency.

2.This protocol withstands the attacks like message coding attack, flow recognition attacks etc.

The disadvantage of this scheme is that,

1.This scheme does not provide destination anonymity.

2.This protocol is prone to DoS attacks, attack by internal adversaries.

**4. ALARM: Anonymous Location Aided Routing:**

One of the a proactive anonymous routing framework ,which maintains the identity privacy, tracks movement of node in hostile and suspicious environment ,is ALARM [4] . Here, a secure MANET map is constructed by taking the current location of the node .Based on the current map, each node decides to whom it wants to communicate.

Group signature is adapted for creating pseudonyms to identify the identity of nodes. The signing process is done by any member of a potentially large and dynamic group. An off-line group manager (GM) initializes the underlying group signature scheme and enrols all legitimate MANET nodes as group members. Mean while, time is divided into different slots of duration T. At the beginning of timeslot, LAM(Location announcement message)is broadcasted by each node. LAM contains GPS coordinates, temporary public key ,time-stamp and a group signature. When the intermediate node receives a message, it checks the group signature to assure its validity. After checking the validity, the node broadcasts the message to its neighbours. A geographical map of MANET is constructed by collecting all the LAMs. When a node needs to communicate to a certain location, it first checks whether there is a node at (or near) that location or not. If so, it sends an encrypted message(by public key) to the destination pseudonym .

The advantages of this protocol is that

1.It can withstand passive insider attack.

The disadvantages of this protocol is that

1.Due to the dynamics of speed, privacy of the node may be compromised.

**5.ASR: Anonymous and Secure Reporting of Traffic Forwarding Activity in Mobile Ad Hoc Networks**

The main objective of this ASR [7] protocol is to provide a secure report on packet forwarding. In this protocol, contribution of intermediate nodes plays an important role in securely transmitting the data traffic. To maintain anonymity in forwarding report, the intermediate nodes are chosen randomly.

The fundamental idea of this protocol is that each intermediate node keeps the track of its own contribution, instead of observing the actions of other nodes. The following three protocols are proposed: Random Reporting Node Selection(RRNS), Random Reporting Node and Direction Selection(RRNDS), and Random Bidirectional Reporting (RBR).

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

*(An ISO 3297: 2007 Certified Organization)*

**Vol. 4, Issue 6, June 2016**

**1.Random Reporting Node Selection(RRNS):** In this protocol, the selection of intermediate node is done randomly by source .Then the intermediate node generates a report and attaches it with the data packet to send it to the destination. The destination observes the activity of intermediate node by receiving those packets.

**2.Random Reporting Node and Direction Selection (RRNDS):**This protocol is proposed to avoid the misinterpretation of location by destination as it receives modified reports from malicious nodes. Here, the chosen node is allowed to decide the direction of sending the report. Piggybacking on reverse path is done for source bound direction.

**3.Random Bidirectional Reporting (RBR):**To avoid source or destination of being shortage of report, this protocol adopts bidirectional reporting ,where source-bound reports are tagged to data packets destined for the source.

The advantages of this protocol are that

1.It efficiently handles eavesdropping attack ,single node misbehaviour.

2. Due to the increase packet size of real time data transmission, this protocol has a small communication overhead .

The disadvantage of this is that,

1.Unidirctional traffic flow is considered in this protocol.

**6.ALERT: An Anonymous Location-Based Efficient Routing Protocol in MANETs**

The Anonymous Location-based Efficient Routing protocol (ALERT) [1] not only offers high security and privacy but also achieves the same at a low cost. This protocol allows network field to partition dynamically into zones and to randomly choose nodes in zones as intermediate relay nodes. ALERT achieves comparable routing efficiency to the GPSR geographical routing protocol.

In this protocol ,hierarchical zone partitioning is adopted ,where data sender partitions the network in order to separate itself and the destination into two zones. Then it splits every partitions into two zones as vertically (or horizontally). Then it randomly chooses a node in the other zone as the next relay node and sends the data to the relay node by using the GPSR algorithm. Then the data is broadcasted to k nodes in the destination zone, providing k-anonymity to the destination. To hide the identity of sender, a number of nodes send information at the same time as the source sends packets. This maintains anonymity in identity of sender.

The advantages of this scheme are that

1.ALERT provides route anonymity, identity, and location anonymity of source and destination.

2. ALERT can also avoid the attacks like, timing attacks because of its non fixed routing paths for a source destination pair.

3.It provides improved data delivery rate.

The disadvantage of this scheme is that

1.This protocol organizes the similar groups in a network, if any one of the node is dishonest the whole group is considered as a dishonest group

**7.An Anonymity-Based Secure On-Demand Routing for Mobile Ad Hoc Networks:**

By adapting group signature scheme and ID based encryption scheme ,this proposed SOT [6] protocol provides user privacy and information security through complete anonymity in an adverse environment . An onion routing is adapted by this scheme which means that, messages are encapsulated in layers of encryption, analogous to layers of an onion. A series of network nodes, known as onion routers, transmit encrypted data, each of which "peels" away a single layer, uncovering the data's next destination. When the final layer is decrypted, the message arrives at its destination. The sender remains anonymous because each intermediary knows only the location of the immediately preceding and following nodes.

The SOT protocol comprises of two phases: first one is initial setup and the then anonymous routing phase. In the first phase, OCM(Offline central manager) provides a group public key and ID-based private key to each user. In anonymous routing scheme ,three subsections are involved such as anonymous key establishment, anonymous route discovery and anonymous data forwarding.

**1.Anonymous key establishment phase**: In this phase, every node obtains the session key anonymously by communicating with its direct neighbour within its coverage area.

**2. Anonymous route discovery Phase:** In this phase, random route pseudonym is established by using cryptographic trapdoor boomerang onion for an on-demand route.

**3. Anonymous data forwarding:** In this phase, the data packets are forwarded by sender anonymously by using outgoing route pseudonym.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

*(An ISO 3297: 2007 Certified Organization)*

**Vol. 4, Issue 6, June 2016**

The advantages of this protocol are that
1. Anonymity is maintained in communication by unlinkability and unobservability.
2.It withstands different attacks like collusion attack, Sybil attack.
3.The packet overhead is less because of sending less control packets.
The disadvantage of this scheme is that
1.Anonymity is not maintained in event reporting.

## III. CONCLUSION

Anonymous routing protocols which provide high security and privacy in MANET has been proposed by this paper. As anonymity is maintained in identity of sender, receiver as well as in rout, many attacks can be prevented from MANET. This survey not only shows the significance but also focuses the limitations of all anonymous routing protocols. This shows that complete anonymous protection in MANET cannot be achieved. So in future work ,the existing protocols can be modified to get high security and privacy in terms of anonymity and to get high performance.

## REFERENCES

1. L. Zhao and H. Shen, "ALERT: An Anonymous Location-Based Efficient Routing Protocol in MANETs," IEEE TRANSACTIONS ON MOBILE COMPUTING, VOL. 12, NO. 6, pp. 304–313 June 2013.
2. Yanchao Zhang, Wei Liu and ,Wenjing Lou, "MASK: Anonymous On-Demand Routing in Mobile Ad Hoc Networks", IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS, VOL. 5, NO. 9, SEPTEMBER 2006
3. J. Kong and X. Hong, "ANODR: Anonymous On Demand Routing with Untraceable Routes for Mobile Adhoc Networks," in 4th ACM International Symposium on Mobile Ad-hoc Networking & Computing (MobiHoc), Annapolis MD, USA, pp. 291-302, 2003.
4. K. E. Defrawy and G. Tsudik, "ALARM: anonymous location-aided routing in suspicious MANETs," IEEE Trans. Mobile Comput., vol. 10, no. 9, pp. 1345–1358, 2011.
5. A. Pfitzmann, and M. Hansen, "Anonymity, Unlinkability, Undetectability, Unobservability, Pseudonymity, and Identity Management – A Consolidated Proposal for Terminology," Draft, February 2008.
6. M. Gunasekaran, K. Premalatha "An Anonymity-Based Secure On-Demand Routing for Mobile Ad Hoc Networks", World Academy of Science, Engineering and Technology, International Journal of Computer, Electrical, Automation, Control and Information Engineering Vol:8, No:1, 2014.
7. C. Heesook, E. William,S.Jaesheungn, D. M. Patrick, and F. L. P. Thomas "ASR: Anonymous and Secure Reporting of Traffic Forwarding Activity in Mobile Ad Hoc Networks", Wireless Networks, pp. 525-539, May- 2009.
8. Boukerche, K. El-Khatib, L. Xu, and L. Korba, "SDAR: a secure distributed anonymous routing protocol for wireless and mobile ad hoc networks," in 29th Annual IEEE International Conference on Local Computer Networks, pp. 618-624, 2004.

## BIOGRAPHY

**A. Naveena** is working as Assistant Professor in the department of ETM, G. Narayanamma Institute of Technology and Science, under JNTU H, Hyderabad ,Telangana. She is also pursuing PhD, under JNTU, Telangana. She received ME degree from OU, Hyderabad, Telangana, India. Her research interests are Wireless sensor networks, MANETs.

**Dr. K. Ramalinga Reddy** is working as Professor, HOD in the department of ETM, G. Narayanamma Institute of Technology and Science, under JNTU H, Hyderabad ,Telangana. He has completed PhD from JNTU H, Telangana. His research interests are Image Processing and Artificial Neural Networks.