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. 3, Issue 1, January 2015

A Survey on Various Manet Routing Protocols Based on Anonymous Communication

Prabhu.K[1], Senthil Kumar.C[2]

PG Scholar, Department of Information Technology, SNS College of Technology, Coimbatore, TamilNadu, India[1].

Assistant Professor, Department of Information Technology, SNS College of Technology, Coimbatore, TamilNadu, India[2].

ABSTRACT: Mobile Ad hoc Networks (MANETs) are a self configurable, Wireless and infrastructure independent network for mobile devices. MANETs have grown to be a challenging and attracting choice for disaster-response and military operations. Due to its ad hoc behaviour of networks, it permits fast operation and doesn't necessitate predefined network infrastructure. In such networks anonymous communications is a challenging topic which permits to exchange messages over communication parties on a network by without disclosing their identifiers of network to each other or to third parties. This type of Anonymous communications can be revealed by means of traffic analysis. Traffic analysis is an advanced approach which exposes relationships between users of anonymous communication systems. In this paper several anonymity enhancing techniques are surveyed for the protection of anonymity communication in mobile ad hoc networks (MANETs). The present survey includes various attacks and its corresponding protocols used for mitigating anonymous communication in MANETs. Finally comparative measures of each method are presented which provides the significance and limitations of each protocol on various attacks in mobile ad hoc networks (MANETs).

KEYWORDS: Anonymous communication, Routing, Mobile ad hoc networks, Energy Efficiency

I.INTRODUCTION

A mobile ad hoc network (MANET) is a continuously self-configuring, infrastructure-less network of mobile devices connected without wires. Ad hoc is Latin and means "for this purpose". Each device in a MANET is free to move independently in any direction, and will therefore change its links to other devices frequently. Each must forward traffic unrelated to its own use, and therefore be a router. The primary challenge in building a MANET is equipping each device to continuously maintain the information required to properly route traffic. Such networks may operate by themselves or may be connected to the larger Internet. They may contain one or multiple and different transceivers between nodes. It results in a highly dynamic, autonomous topology MANETs are a kind of Wireless ad hoc network that usually has a routable networking environment on top of a Link Layer ad hoc network. MANETs consist of a peer-to-peer, self-forming, self-healing network in contrast to a mesh network has a central controller. MANETs circa 2000-2015 typically communicate at radio frequencies (30 MHz - 5 GHz). Multi-hop relays date back to at least 500 BC.

The growth of laptops and 802.11/Wi-Fi wireless networking have made MANETs a popular research topic since the mid-1990s. Many academic papers evaluate protocols and their abilities, assuming varying degrees of mobility within a bounded space, usually with all nodes within a few hops of each other. Different protocols are then evaluated based on measures such as the packet drop rate, the overhead introduced by the routing protocol, end-to-end packet delays, network throughput, ability to scale. Mobile ad hoc networks (MANETs) have been developed into one of the fastest growing parts of research by means of its smaller, cheaper, and more powerful mobile devices. Due to the flexibility afforded by its dynamic infrastructure, MANETs are considered as attractive and advanced technology for various applications namely military, disaster-response, tactical and rescue operations. This new kind of infrastructure free network merges wireless communication along with high degree node mobility During the last two decades, research in various aspects of mobile ad-hoc networks (MANETs) has been very active, motivated mainly by military, disaster relief and law enforcement scenarios. More recently, location information has become increasingly available through small and inexpensive GPS receivers, partially prompted by the trend of introducing location-sensing capabilities into personal handheld devices .A natural evolutionary step is to adopt such locationbased operation to

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. 3, Issue 1, January 2015

MANETS. This results in what we term location-based MANETS. In such a MANET, devices rely on location information in their operation. The main distinguishing feature of the envisaged location-based MANET environment is the communication paradigm based not on permanent or semi-permanent identities, addresses or pseudonyms, but on instantaneous node location.Traditional wired networks employ dedicated nodes to perform fundamental functions namely routing, packet forwarding and network management. Nodes on MANET's employ multi-hop communication that is nodes which are within other radio range may communicate via wireless links, whereas nodes that are at distant might rely on intermediate nodes which perform as routers to transmit messages. Due to the dynamic network topology, mobile nodes can migrate, disappear and links the network by frequently updating its routes. Anonymity is a property of network security.

An entity in a system has anonymity if no other entity can identify the first entity, nor is there any link back to the first entity that can be used, nor any way to verify that any two anonymous acts are performed by the same entity. It includes, A)Unlinkability of sender and receiver B)Route discovery C)Data delivery D)Modifying control functions E)Trust management The following literature surveys anonymous communication. And merits and demerits of each method are represented in the comparative table which is described in the following section

.

II.RELATED WORK

An extensive literature survey has been done to analyze the performance of routing protocols for various mobility models. Few researchers have carried out experiments to study the performance of reactive routing protocols such as DSR and AODV in mobile environments .The traffic patterns perform an important role in the performance of routing protocols. The more commonly know protocols such as AODV, DSR , were proposed to provided more efficient routing in a wireless environment. The protocols were mainly evaluated for packet delivery ratio and routing overhead. Recently, multimedia applications have drawn the attention of researchers a lot in MANET. There are a numerous protocols addressing the issue of routing in MANETs, routing becomes a challenge as the nodes are mobile, thus resulting in loss of packets, delay and inefficient communication. Also the problem of insecure wireless links poses a threat to communication in MANETs. The data rate in voice application increases till it reaches a maximum peak. All of the above mention protocols provide security. Besides security; privacy is also an important issue that needs equal attention. Privacy not only refers to confidentiality of the information being passed but also is the property of nodes to remain undetectable by adversaries.

III. ANALYSING VARIOUS ROUTING PROTOCLS IN MANET BASED ON ANONYMOUS COMMUNICATION

A.Anonymous on- Demand routing protocol

In [1] Jiejun et.al presented anonymous routing protocol known as Anonymous On-Demand Routing (ANODR) as the countermeasure. In real time, ANODR is a merely on-demand routing system that presently sets up desired anonymous routes. This restricts the possibility of traffic analyzing and eavesdropping to a critical time on-demand window. Generally in a mobile environment, few options are left for the adversary in whom they can instigate the attack in the critical time window or its corresponding information about the out-of-date of the protected mobile nodes. An additional characteristic of ANODR is that it is the original identity-free ad hoc routing system, which is divergent to all earlier ad hoc routing system derived from node identities like MAC addresses and IP. In place of using node identities, one-time cryptographic trapdoors are relied on ANODR in routing. By without knowing node identities, the adversary cannot break a node's identity anonymity of mobile excluded by way of intrusion of node. This creates an immense physical dispute to the adversary.

B.MANET Anonymous Peer-to-peer Communication Protocol

In [2] Chao-Chin presented MANET Anonymous Peer-to-peer Communication Protocol (MAPCP), for peer to peer applications over mobile ad-hoc networks. This protocol is considered to be a flexible middleware connecting the MANET routing protocols and peer to peer applications. MAPCP utilizes a broadcast based method jointly with a probabilistic-based flooding control algorithm to launch anonymous paths among peers, which involves no hop-by-hop encryption or decryption, therefore entails lower power consumption and computational complexity. This protocol launches several anonymous paths among communication peers exist in a single phase of query, and is extremely

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. 3, Issue 1, January 2015

resilient to node failure, mobility and malicious attacks. Moreover, MAPCP offers plans for communication peers to manage the trade off involving bandwidth efficiency and anonymity degree.

C.Energy Efficient, Secure and Stable Routing Protocol

In [3] Sunil et.al presented Energy Efficient, Secure and Stable Routing Protocol, ad hoc network holds the hosts communicating between themselves with moveable radios. Due to the limited radio propagation range of this network which can be organized by without considering any infrastructure support or wired base station where routes are primarily considered as multi-hop. The ad hoc network nodes are limited by battery power for their function. A sufficient number of intermediate nodes are used to route a packet from a source to a destination. An efficient resource is said to be Battery power of a node which need to be employed proficiently so as to keep away from early termination of a network or a node. One unique characteristic of Energy Efficient ad hoc routing protocol is its exploitation of Power for each entry of route. For a certain option to reach a destination by means of two routes, a demanding node is essential to choose one with improved power status.

D.Anonymous Location-based Efficient Routing protocol

In [4] Haiying et.al presented Anonymous Location-based and Efficient Routing protocol (ALERT) for traffic analysis in MANET. ALERT forms a nontraceable anonymous route by dynamically splitting a network range into zones and arbitrarily decides nodes in zones as intermediate relay nodes. Particularly, in each step of routing, a data sender divides the network environment so as to split themselves and the destination into two zones. After that it randomly picks a node in the rest zone as the subsequent relay node and employs the GPSR algorithm to forward the data to the relay node. Finally, the data is transmitted to k nodes in the zone of destination by offering k-anonymity to the destination node. Additionally, ALERT has a scheme to conceal the data originator between a amount of initiators to reinforce the anonymity defence of the source node. Furthermore ALERT is resilient to timing attacks and intersection attacks.

E.Onion Routing Protocol

In [5] Michael.et.al presented onion routing prototype which can be employed to protect an Internet services against both traffic analysis attacks and eavesdropping from both the outside observers and network. They split the connection anonymity from the communication anonymity over that connection. For instance, when two parties operating onion routers which is able to recognize themselves to each other by without disclosing the existence of a connection between them. This work examines the adaptability of anonymous connections by extending their use in a various Internet applications. These applications comprise standard Internet services such as electronic mail, Web browsing and remote login. In addition Anonymous connections have also been used to hold virtual private networks (VPN) with connections that are opposing to traffic analysis which holds connectionless traffic. For supporting anonymous connections the configuration of onion routing network can be handled in different ways which includes customer-ISP configuration and firewall configuration, shifts privacy to the user's computer and may ease the carrier of responsibility for the user's connections.

F.MASK

In [6] Yanchao et.al presented framework of a new anonymous on-demand routing protocol, known as MASK, which can concurrently attain anonymous MAC-layer and network-layer communications. The originality of MASK relies in the exploitation of dynamic pseudonyms quite rather than network addresses and static MAC. MASK suggest anonymity of sender and receiver plus relationship anonymity of sender-receiver. Particularly, even if adversaries might examine a transmission of packets in which they neither establish real network IDs of its sender and receiver, nor they choose when some two nodes are communicating in the network. Additionally, MASK guarantees node as untrackability and unlocatability sense that, even though adversaries might identify some real network IDs or its group memberships, they are not capable to make a decision whom and where the related nodes are in the network. Furthermore, MASK warranties end-to-end flow untraceability, sense that forwarded packets are not traced by adversaries to its ending destination or backward to its new source, In addition they cannot identify packets corresponding to a original communication flow.

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. 3, Issue 1, January 2015

G.ARM Protocol

In [7] Stefaan Seys and Bart Preneel proposed the ARM protocol. It requires no cryptographic operations in order for nodes to be able to recognize a message as being targeted at them or not. Nodes that only participate in the hiding process only need to decrypt and encrypt the short message header using their broadcast keys. Assume that every node in the network has a permanent identity that is known by the other nodes in the network that wish to communicate with this node. Assume that the source S and the targeted destination D share a secret key kSD and a secret pseudonym. The source will include this pseudonym in RREQ messages targeted at this specific destination. Once the source of a RREQ message receives a RREP message with the same identifier NymSD, it can start sending DATA messages to the destination. Similar to sending RREQ messages, DATA messages will have a onetime identifier attached to them.
It allows a node on the route to recognize the fact that it is the next hop and that it should forward the message. Forwarding DATA messages is similar to forwarding RREP messages, using the same ttl scheme, but no padding is required. For the RREP messages the source chooses a random padding length with a uniform probability distribution between zero and some maximum Nodes forwarding a RREP message keep the length of the RREP message constant by adding padding the size of the peeled of layer to the end of the RREP message before forwarding it. ARM protocol Anonymity is an important part of the overall security architecture for mobile ad hoc networks as it allows users to hide their activities. It enables private communications between users while making it harder for adversaries to focus their attacks

H.Temporary Ordered Routing Protocol(TORA)

. In[8]TORA is a distributed highly adaptive routing protocol designed to operate in a dynamic multihop network. TORA has four basic functions: route discovery, route maintenance, route erasing, and route optimization. TORA uses an arbitrary height parameter to determine the direction of link between any two nodes for a given destination. Consequently, multiple routes often exist for a given destination but none of them are necessarily the shortest route. To initiate a route, the node broadcasts a QUERY packet to its neighbors. This QUERY is rebroadcasted through the network until it reaches the destination or an intermediate node that has a route to the destination. The recipient of the QUERY packet then broadcasts the UPDATE packet which lists its height with respect to the destination. When this packet propagates in the network, each node that receives the UPDATE packet sets its height to a value greater than the height of the neighbor from which the UPDATE was received. This has the effect of creating a series of directed links from the original sender of the QUERY packet to the node that initially generated the UPDATE packet

IV.COMPARATIVE ANALYSIS

The following comparative table provides the merits and demerits of each surveyed method as follows:

Table -1: Comparison of Algorithms

s. no	Title	Protocol Used	Merits	De-Merits
1	An Identity-Free And On Demand Routing Scheme Against Anonymity Threats In Mobile Ad-Hoc Networks	Anonymous on-Demand routing protocol (ANODR)	Better trade-offs between routing performance and security protection is obtained.	Performance of routing varies significantly when different cryptosystems are utilized. It does not focus on security. It have less efficiency.
2	An Efficient Anonymous Communication Protocol For Peer-To-Peer Applications Over Mobile Ad-Hoc Networks	MANET Anonymous Peer-to-peer Communication Protocol (MAPCP)	Results in lower computational complexity and power Consumption, Resilient to passive Attacks, Achieves a high anonymity degree	Overhead delay is high.

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. 3, Issue 1, January 2015

3	Energy efficient, secure and stable routing protocol for MANET.	Sunil Taneja and Ashwani Kush. May 2012	Energy Efficient, Secure and Stable Routing Protocol (EESRP)	Provides energy efficient, secure and stable routing strategy for MANETS, It is simple and flexible.
4	Alert: An Anonymous Location Based Efficient Routing Protocol in MANET	Anonymous Location-based Efficient Routing protocol (ALERT)	Offer high anonymity protection at a low cost, Achieve comparable routing efficiency.	Not resilient to active attacks.
5	Anonymous Connections And Onion Routing	Onion routing network prototypes.	• Efficiently analyses the traffic. • It provides protection against eavesdropping as a side effect.	Improved throughput is not obtained
6	MASK: Anonymous on-demand routing in mobile ad-hoc networks	MASK	Preserves the high routing efficiency, Highly effective and efficient	The final destination is contained within every RREQ message in plain text. MASK relies on a tight synchronization of keys and pseudonyms between neighbouring nodes.
7	Arm: anonymous routing protocol for MANET	ARM Protocol	It provides stronger anonymity properties High efficiency	It does not provide security to the network.

V.RESULTS

The present survey paper discussed the various kinds of MANET routing protocols where their performance is measured in op-net simulator and their advantages and disadvantages are discussed in this paper. Each surveyed method is significantly efficient in terms of its corresponding performance metrics and resilient to various characteristics. Table I in the Appendix compares the various routing protocols of MANET with its merits and demerits and the type of protocols used. The above protocols are best for the anonymous communication in which MASK and EESRP protocols are energy efficient than other protocols of MANET. Onion routing protocol performs better than the other routing protocols of MANET.

VI.CONCLUSION

The present survey presents various attacks and its corresponding protocols used for mitigating anonymous communication in MANETs. Each surveyed method is significantly efficient in terms of its corresponding performance metrics and resilient to various attacks. The presented literature shows the pros and cons of each method in various aspects. The efficiency of the surveyed method can be measured in terms of computational time, power consumption, computational complexity, overhead and throughput respectively.

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. 3, Issue 1, January 2015

REFERENCES

1. J. Kong, X. Hong, and M.Gerla, "An Identity-Free and On- Demand Routing Scheme against Anonymity Threats in Mobile Ad Hoc Networks," IEEE Trans. Mobile Computing, VOL. 6, NO. 8, PP. 888-902, AUG. 2007.
2. Chao-Chin Chou, David S. L. Wei, C.-C. Jay Kuo, and Kshirasagar Naik,"An efficient Anonymous communication protocol for peer to peer applications over Mobile Ad-hoc networks" IEEE Trans.Communication,VOL 25, NO, 1, 2007.
3. Sunil Taneja & Ashwani Kush," Energy Efficient, Secure and Stable Routing Protocol for MANET", Global Journal of Computer Science and Technology, VOLUME 12 ISSUE 10 VERSION 1.0,2012
4. Haiying Shen, and Lianyu Zhao," ALERT: An Anonymous Location-Based Efficient Routing Protocol in MANETs", IEEE TRANS. MOBILE COMPUTING, VOL. 12, NO. 6, 2013
5. M. Reed, P.Syverson, and D.Goldschlag, "Anonymous Connections and Onion Routing," IEEE J. Selected Areas in Comm., VOL. 16, NO. 4, PP. 482-494, MAY 2002.
6. Y. Zhang, W. Liu, W. Lou, and Y. Fang, "MASK: Anonymous On-Demand Routing in Mobile Ad Hoc Networks," IEEE Trans.Wireless Comm., VOL. 5, NO. 9, PP. 2376-2385, SEPT. 2006.
7. S. Seys and B. Preneel, "ARM: Anonymous Routing Protocol for Mobile Ad Hoc Networks,"Proc. IEEE 20th Int'l Conf. Advanced Information Networking and Applications Workshops (AINA Workshops '06),PP. 133-137, 2006.
8. Gurpinder Singh, Asst. Prof. Jaswinder Singh," MANET: Issues and Behavior Analysis of Routing Protocols" International Journal of Advanced Research in Computer Science and Software Engineering, Volume 2, Issue 4, April 2012.