www.ijemr.net ISSN (ONLINE): 2250-0758, ISSN (PRINT): 2394-6962

Vandana Publications
IJEMR

Volume-5, Issue-3, June-2015
International Journal of Engineering and Management Research
Page Number: 267-270

Anonymous Routing Protocols for MANETs-A Survey

Chaitanya Bajantri[1], Mr.Shreekant S[2]
[1]M. Tech(CNE), Department of CSE, S.I.E.T, Vijayapura, INDIA
[2]Professor, Department of CSE, S.I.E.T, Vijayapura, INDIA

ABSTRACT

A Mobile Ad Hoc Network (MANET) is a self-organizing network of mobile nodes. In most cases the nodes communicate to each other based on public identities. But while considering application such as military, nodes should not expose their identities and node activities must not be visible. MANET s use anonymous routing protocols that hide node identities and/or routes from outside intruder or attackers in order to give anonymity protection. Although a number of anonymous secure routing protocols have been proposed, the requirement is not fully satisfied. The existing protocols are susceptible to the attacks of routing packets or denial-of-service (DoS) broadcasting, even though node identities are sheltered by pseudonyms.

Keywords—MANETS, Delay, Anonymit, Pseudonyms.

I. INTRODUCTION

The term MANET (Mobile Ad hoc Network) is referred to as multihop packet based wireless network which consists of a set of mobile nodes that can communicate and move at the same time, not using any type of fixed wired infrastructure. MANET is actually self organizing and adaptive networks that can be formed and deformed on-the-fly without the need of any centralized administration. Otherwise, a stand for "Mobile Ad Hoc Network" A MANET is a type of ad hoc network that can change locations and configure itself on the fly. Because MANETS are mobile, they use wireless connections to connect to different networks. This can be a standard Wi-Fi connection, or another medium, such as a cellular or satellite transmission.

Ease of An ideal anonymous routing protocol for MANETs should have the following properties:
(1) The topological information of the network should not be exposed. Accessing to them renders the system susceptible to attacks.
(2) The identities and locations of the nodes in the route, should be protected.
(3) Multiple paths should be established to increase the difficulty of traffic analysis and avoid broken links due to node mobility.

To implement anonymous communications there is need to propose appropriate secure routing protocols.To build up the anonymous protocols a direct method is used to annoymize commonly used on ad hoc routing protocols , such as AODV[16] and DSR[17] . For this purpose, we need to provide anonymous security features to the source, destination, and every intermediate node along a route.

II. LITERATURE SURVEY

This section describes already existing technologies. Literature survey conducted provides the results that helps to propose and implement new work correctly by overcoming most of the disadvantages that are present in the existing work.

A. ANonymous On Demand Routing With Untraceable Routes for Mobile Ad hoc networks

In unfriendly environments, the enemy can start analyzing the traffic against interceptable routing information is well established in routing messages and data packets. Allowing adversaries to trace network routes and identify the motion pattern of nodes at the end of those routes may cause a serious risk to secret operations. The protocol ANODR, an anonymous on-demand routing protocol for mobile ad hoc networks deployed in hostile environments. We address two closely related problems: For route anonymity, ANODR limits strong adversaries from tracing a packet flow from source to destination and vice versa; for location privacy, ANODR guarantees that the real identities of local transmitters cannot be realize by adversaries. The design of ANODR is based on "broadcast with trapdoor information", a network security concept which includes features of two existing network and security mechanisms, namely "broadcast" and "trapdoor information". Disadvantage of this approach is it can only prevent outside passive attackers.

B. A Secure Distributed Anonymous Routing Protocol for Wireless and Mobile Ad hoc Networks

Providing security and privacy in mobile ad hoc networks has been a main question over the last few years. Most research work has so far given attention on providing security for routing and message content, but nothing has been done in regard to providing privacy and anonymity over these networks. The protocol, SDAR which doesn't use temporary or continuously changing identities. Instead SDAR uses a single permanent identity for every node. Every intermediate node inserts its identity as the source address of every message it broadcast. It requires every forwarding node to carry out a public key decryption, a public key encryption and a signature creation for every Route request message. It forwards protocol does not require the source node to collect and store information about the network topology.

C. Ad-Hoc On-Demand Position-Based Private Routing Protocol

AO2P works in the network with relatively high node densities, where the positions of destinations are the only position information disclosed in the network for routing. In A02P, discovery of route is done by sending a routing request message from the source to the location of the destination. In A02P, once a prior hop sends out a routing request, the neighboring nodes who receive the request will contend to access the channel to be the next hop. In the receiver contention mechanism, different classes have been assigned for different receiving nodes according to how close they can bring the routing request towards the destination. The class is been assigned with high priority for the receiver which is geographically closer to the destination, and it normally can win the contention. This gives the routes with a minimum number of hops. less forwarders are needed and, hence, the channel is shared by fewer nodes. These routes generally have a better routing performance in a network with a fixed data rate. Once a route is built, temporary MAC and pseudo IDS addresses are used for the nodes in the routes, such as sources, destinations, and intermediate forwarders. Since the identities of the nodes are not disclosed, anonymity in communication can be achieved. Eavesdroppers only know that at a certain position the node will receive data, but they do not know which node it is. The disadvantage of this protocol is delay produced by the proposed contention method.

D. Anonymous On-Demand Routing in Mobile Ad hoc Networks

The anonymous authentication with low cryptographic overhead and high routing effectiveness can be obtained by using proactive neighbor detection. It is opposition to a wide range of adversarial attacks. MASK relies on a proactive neighbor detection protocol to constantly see the snapshot of its one-hop mobile neighborhood. MASK’s neighbor detection protocol is identity-free. The physical presence of neighboring nodes is known by each MASK node. This is achieved by a pairing-based anonymous handshake between neighboring nodes of any pair. MASK uses a three-stage handshake for key exchanges among a node and its new neighboring nodes. After the handshake, each pair of nodes shares locally unique LinkID pair which correspond to the pseudonyms used during handshake and a chain of secret key. MASK does not use a global trapdoor. In the MASK’s RREQ packet, source S explicitly puts in the destination node D’s network ID. This saves the processing overhead to open the global trapdoor, thus cautious the need of end-to end key conformity and results in a more capable RREQ procedure. However, the security trade-off is that recipient anonymity is compromised by every RREQ receiver. The routing information is not real. Already established path may consist of several multipath channels however the source and the destination nodes become unreal. Drawback is there is no destination anonymity.

E. Discount anonymous on demand routing for mobile ad hoc networks

Here it is provided the similar mechanism of ANODR, but at a lesser cost. It uses the same approaches used in ANODR. They provided end-to-end privacy of both payload and control messages using a cryptographically trivial protocol relying exclusively on symmetric cryptography for its process .It has the advantage of achieving substantially lower calculation and communication complexities at the cost of a slight less of security guarantees. Route requests in Discount-ANODR allow strong similarities to the Route request in ANODR with the limitation that intermediaries only know the destination of the request and the identity of the previous intermediary but not the originator of the request.

F. Anonymous Authentication Protocol In MANETS

They have proposed distributed reputation system. This reputed distributed system is included with trust management. It controls activity of nodes being along the path and evaluate their level of trust. Reputation depends upon own past experience, time, second hand information and it is expressed by level of trust. The end to end anonymous authentication is conducted in three-phase. The three phases are anonymous. Authentication initialization, anonymous reply, and anonymous authentication. After the successful authentication multiple anonymous data channels are established. A computational overhead and node’s capabilities constrains is a big challenge for security design in MANETS.

G. Efficient Anonymous Dynamic Source Routing for Mobile Ad-Hoc Networks

This paper provides three levels of security protection. This routing consists of three protocols. The first protocol is used to generate shared key and a nonce between the source and the destination for the protected communication. The second protocol uses the shared key and the nonce to create a trapdoor and employ anonymous onion routing between the source and the destination. In the last protocol the source and the destination uses their session key shared with the intermediate nodes to encrypt all communications with the cryptographic onion method. It offers good scalability. The anonymous route establishment depends on the number of hops between the source and the destination, if number of hops increases time will be also increased.

H. Anonymous Routing protocol for mobile ad hoc networks

Here the source and the destination share a secret key KSD and a secret assumed name. The source will include this assumed name in the route request message. The destination will have a list of assumed name used by different sources in its memory and it verifies whether the message is targeted at it or not. This assumed name can be used only once. The destination sends the reply with the same assumed name. On the receipt of the reply message source starts to send the data along with the one time identifier attached with them. One time identifier protects the data from the intruder. Delay increases when the network size is large.

I. Anonymous Location-Aided Routing in Suspicious MANETs

It uses current positions of the node to securely broadcast and construct snapshots of the topologies and forward data. It uses advanced cryptographic techniques (e.g., group signatures). ALARM relies on group signatures to construct one-time pseudonyms used to identify nodes at certain locations. ALARM provides both privacy and security features, including data integrity, node authentication, and untraceability (tracking-resistance). Although it doesn't provide full security on the location anonymity of source and destination due to the dynamics of the speed and the mobility patterns of nodes inside the MANET.

J. An anonymous location-based efficient routing protocol in MANETS

Here in this protocol dynamically partitioning of the network field into zones will takes place. And in zones it will randomly chooses the nodes as intermediate relay nodes, which form non observable anonymous route. In addition, it hides the data originator/recipient among many originators/recipients to improve source and destination anonymity protection. ALERT offers anonymity protection to sources, destinations, and routes. In each routing step, in order to separate itself and the destination into two zones, a data sender or forwarder partitions the network field . It then randomly chooses a node in the other zone as the next relay node and uses the GPSR algorithm to transmit the data to the relay node. In the last step, the data is broadcasted to k nodes in the destination zone, providing k-anonymity to the destination. A notify and go mechanism is integrated in order to have the source anonymity. Disadvantage of proposed work is ,it does not consider the active internal intruders.

K. Achieving Efficient Anonymity in MANETS by Combining HIP, OLSR, and Pseudonyms

The protocol HOP is based on cryptographic Host Identity Protocol (HIP) which provides security and user level anonymity. Some enhancement is done to the authentication process to achieve Host Identity Tag (HIT). HIP protocol is combined with OLSR routing protocol to achieve the support for pseudonym. It uses multiple IP addresses per station to achieve a higher degree of anonymity when communicating. When two nodes wish to establish a secure connection, each will select a free IP address from its IP address pool that is used as a pseudonym for that connection. This approach is lightweight and it is easy to implement. It maximizes the performance. The maximum data encryption rate was limited to 12 M bit/s.

III. PROPOSED SYSTEM

Techniques used are:

1. Trapdoor

In cryptographic functions [13], a trapdoor is a general notion that defines a one-way function between two sets. A universal trapdoor is an information collection process in which in-between nodes may add information elements, such as node IDs, into the trapdoor.

2. Group Signature

This scheme [21] is used to provide authentication for the members in the network. Group manager issues a pair of group public and private keys to each and every member in a group

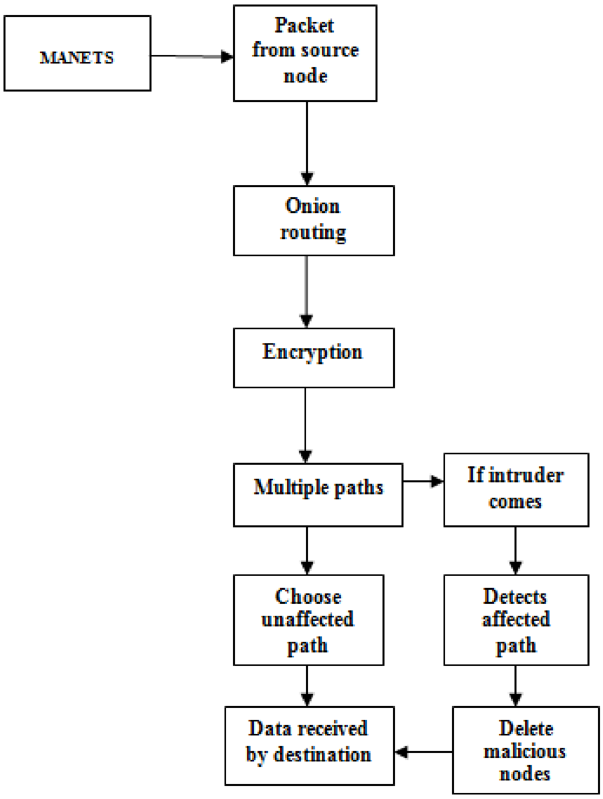

Fig 1.Block Diagram of Proposed System

3. Onion Routing

It is a technique [14] to provide secure communications over a public network. The source node sets up the central part of an onion with a specific route message. During a route request phase, each forwarding node decrypt layer of the route request message.

As shown in Fig 1,first the MANET is created, the nodes starts to sense the data. To transmit the data first the data is encrypted and sent to the destination through the intermediate nodes using Onion routing algorithm. It will choose multiple paths to send data. Now if any attacker comes in the path and the path is affected then the affected path will be deleted, and the data will be sent to the destination through unaffected path securely.

IV. CONCLUSION

The anonymous routing protocols which are discussed in the literature survey focus only on providing anonymous protection to the data sources, destination, routes. Most of the anonymous routing protocols provides anonymous protection with increase in delay. The proposed system supports multiple paths for data transfer,if one path affected by the attacker then it will choose one among the remaining two paths for data transfer and hence the delay is reduced .

REFERENCES

[1] J. Kong and X. Hong, "ANODR: ANonymousOn Demand Routing with Untraceable Routes for Mobile Ad hoc networks," in Proc. ACM MobiHoc'03, Jun. 2003, pp.291–302.

[2] A. Boukerche, K. El-Khatib, L. Xu, and L. Korba, "SDAR: a Secure Distributed Anonymous Routing Protocol for Wireless and Mobile Ad hoc Networks," in Proc. IEEE Int'l Conf. Local Computer Networks (LCN'04), Nov. 2004, pp. 618–624.

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

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

[5] L. Yang, M. Jakobsson, and S. Wetzel, "Discount anonymous ondemand routing for mobile adhoc networks," in Proc. Int. Conf. on SECURECOMM'06, Aug. 2006.

[6] Tomasz Ciszkowski Zbigniew Kotulski, "ANAP: Anonymous Authentication Protocol In MANETS," Warsaw University of Technology, 2006.

[7] Ronggong Song, Larry Korba, George Yee" AnonDSR: Efficient Anonymous Dynamic Source Routing for Mobile Ad-Hoc Networks", Proceedings of the 2005 ACM Workshop on Security of Ad Hoc and Sensor Networks, 2007.

[8] S. Seys and B. Preneel, "ARM: Anonymous Routing protocol for mobile ad hoc networks," Int. Journal of Wireless and Mobile Computing, vol. 3, no. 3, pp. 145–155,Oct. 2009.

[9] 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.

[10] H. Shen and L. Zhao, "ALERT: An Anonymous Location-based Efficient Routing Protocol in MANETs,"IEEE Trans. on Mobile Computing, vol. 12, no. 6, pp.1079–1093, 2013.

[11] 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.

[12] J. Paik, B. Kim, and D. Lee, "A3RP: Anonymous and Authenticated ad hoc Routing protocol," in Proc. International Conf. on Information Security and Assurance (ISA'08),Apr. 2008.

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

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

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

[16] C. Perkins, E. Belding-Royer, S. Das, et al., "RFC 3561 – Ad hoc On-Demand DistanceVector (AODV) Routing," Internet RFCs, 2003.

[17] D. Johnson, Y. Hu, and D. Maltz, "RFC 4728 – The Dynamic Source Routing Protocol (DSR) for Mobile Ad Hoc Networks for IPv4," Internet RFCs, 2007.

[18]Aarti ,Dr. S. S. Tyagi, "Study of MANET: Characteristics,Challenges, Application and Security Attacks" Volume 3,Issue 5, May 2013.

[19] http://www.isi.edu/nsnam/xgraph/ XGraph homepage

[20]http://www.geocities.com/tracegraph/TraceGraph

[21] Subhra Mishra ,Tilak Rajan Sahoo, " A Survey onGroup Signature Schemes", Department of Computer Science and Engineering National Institute of Technology Rourkela 769 008, India.