Efficient Anonymous Routing Protocols in Manets: A Survey

Jojy Saramma John[#1], R.Rajesh[#2]

[1]Student, Computer Science and Engineering, Vivekanadha Institute of Engg & Tech for Women, Erode, India

[2]Assistant Professor, Computer Science and Engineering, Vivekanadha Institute of Engg & Tech for Women, Erode, India

***Abstract*— Mobile Ad Hoc Networks (MANETs) use anonymous routing protocols that hide node identities and/or routes from outside observers in order to provide anonymity protection. Anonymity in MANETs includes identity and location anonymity of data sources (i.e., senders) and destinations (i.e., recipients), as well as route anonymity. Existing anonymity routing protocols in MANETs can be mainly classified into two categories: hop-by-hop encryption and redundant traffic routes. In this paper ,we study and compare between the existing anonymous routing protocols deployed for MANETS..**

***Keywords*— MANET, survey, anonymity, routes;**

I. Introduction

Ad hoc network is a self-organizing multi-hop wireless network, which relies neither on fixed infrastructure nor on predetermined connectivity. ad hoc network is considered to be different from other networks as they are defined to be highly deployable, reconfigurable and constitute high mobility ,low bandwidth and lack of centralized entity. ad hoc networks are classified based on various parameters such as symmetric and asymmetric characters, traffic characteristics, routing methods, time and reliability constraints. manet is a infrastructureless type of ad hoc network which is rapidly deployable and self-configuring .manet is a standalone network in which nodes are mobile and topology is dynamic. manet usage extend to areas like military scenarios ,sensor networks ,rescue operations, students on campus, conferences etc. to standardize ip routing in mobile ad hoc network, routing protocols are accepted that fall in three categories: reactive(on-demand) routing protocol, proactive(table driven) protocol and hybrid protocol. nodes in manets are vulnerable to malicious entities that aim to tamper and analyze data and traffic analysis by communication eavesdropping or attacking routing protocols.

Anonymous routing protocols are crucial in manets to provide secure communications by hiding node identities and preventing traffic analysis attacks from outside observers. anonymity in manets includes identity and location anonymity of data sources (i.e., senders) and destinations (i.e., recipients), as well as route anonymity. “identity and location anonymity of sources and destinations” means it is hard if possible for other nodes to obtain the real identities and exact locations of the sources and destinations. for route anonymity, adversaries, either en route or out of the route, cannot trace a packet flow back to its source or destination, and no node has information about the real identities and locations of intermediate nodes en route. also, in order to dissociate the relationship between source and destination (i.e., relationship unobservability, it is important to form an anonymous path between the two endpoints and ensure that nodes en route do not know where the endpoints are, especially in manets where location devices may be equipped. existing anonymity routing protocols in manets can be mainly classified into two categories: hop-by-hop encryption and redundant traffic . in hop-by-hop encryption routing, a packet is encrypted in the transmission of two nodes en route, preventing adversaries from tampering or analyzing the packet contents to interrupt the communication or identify of the two communicating nodes. hop-by-hop encryption routing can be further divided into onion routing and hop-by-hop authentication. in onion routing, packets are encrypted in the source node and decrypted layer by layer (i.e., hop by hop) along the routing path.

II. PRIVACY FACTORS OF MANETS

The key notations of privacy associated with MANETS are summarized as follows:

Identity privacy: Identity privacy means no one knows the real identity of nodes in network .Identity privacy of entities involves in packet transmission are source, intermediate nodes and destination.

Location Privacy: Requirements for location privacy are as follows: (a) no one knows the exact location of a source and destination, except themselves (b) intermediate nodes does not know the distance.

Route Anonymity: Requirements for route anonymity are as follows : (a) adverseries in the route or out of the route cannot trace packet flow back to source or destination (b) adverseries not in the route have no information on any part of the route.;(c)difficult for adverseries to infer packet transmission.

Attacks on MANETS are categorized as passive and active attacks:

Passive attacks: Passive attacks typically involves unauthorized listening to the routing packets or silently refusing unauthorized execution of function requested. This type of attack may be an attempt to gain routing information about the positions of each node in relation to each other. This type of attack is usually difficult to detect as they does not disrupt routing protocol but only tries to discover valuable information.

Active attacks: Active attacks are meant to degrade or prevent message flow between nodes. Such attacks involve actions like replication, modification and deletion of data. These cause complete degradation or complete halt in communication between nodes. Examples of such attacks are :

DoS: Multiple adverseries in corporation or one adversary with enough power can set a specific node as target node in order to exhaust the resource of that node. That is to identify a node and make a target to that node.

Wormhole attack: In wormhole attack, the attacker records a packet at one location of the network and sends it to other location of the network through a tunnel made between attacker nodes.

Rushing attack: Existing on demand routing protocol forwards a request packet that arrives first in each route discovery. In the rushing attack, the attacker exploits the property of route discovery operation. In general attacker can forward a route request more quickly than legimate nodes can,so he can enter a route. Such a route cannot be easily detected.

III. PROACTIVE ROUTING PROTOCOLS

A.ALARM:ANONYMOUS LOCATION AIDED ROUTING PROTOCOL

A framework for Anonymous Location-Aided Routing in MANETs (ALARM) demonstrates the feasibility of obtaining, at the same time, both strong privacy and strong security properties. By privacy properties we mean node anonymity and resistance to tracking. Whereas, security properties include node/origin authentication and location integrity.

ALARM involves the following assumptions:

Location: Each MANET node can securely and reliably obtain its present position, most likely via GPS.

Time: ll MANET nodes maintain loosely synchronized clocks. This is easily obtainable with GPS.

Range: all nodes have uniform transmission range. Once a node knows the current MANET map, it can easily determine node connectivity (i.e.,transform a map into a graph)

Mobility at least *K* nodes move at roughly the
same time, i.e., within a certain fixed time period.

The basic operation of ALARM is as follows:

Time is divided into time slots of duration *T*. At the beginning of every slot, each node broadcasts a message containing: its location (GPS coordinates), time-stamp, temporary public key and a group signature computed over these fields. This a called **Location Announcement Message (LAM)**. Each LAM is flooded throughout the MANET In the period between successive LAM-s, a node can be reached using a pseudonym which is set to the group signature in its last LAM. Each node that receives a LAM, first verifies the group signature. If the signature is valid, the node broadcasts the message to its neighbors unless it has previously received the same message. Having collected all current LAM-s, each node can easily construct a geographical map and a connectivity graph of the MANET.

If a node needs to communicate to a certain location ,it first checks to see if there is a node at (or near) that location. If so, it sends a message to the destination pseudonym (determined by the group signature in the last LAM corresponding to that location). The message is encrypted with the public key included in the same LAM. The ALARM framework supports anonymous location-based routing in certain types of suspicious MANETS.

ALARM relies on group signatures to construct one-time pseudonyms used to identify nodes at certain locations. The framework works with any group signature scheme and any location-based forwarding protocol can be used to route data between nodes. if a portion of the nodes are stationary, or if the speed of movement is not very high.

B.ALERT:ANONYMOUS LOCATION EFFICIENT ROUTING PROTOCOL

Previous anonymous routing protocols, relying on either hop-by-hop encryption or redundant traffic, generate high cost. Also, some protocols are unable to provide complete source, destination, and route anonymity protection. ALERT is distinguished by its low cost and anonymity protection for sources, destinations, and routes. It uses dynamic hierarchical zone partitions and random relay node selections to make it difficult for an intruder to detect the two endpoints and nodes en route.

A packet in ALERT includes the source and destination zones rather than their positions to provide anonymity protection to the source and the destination. ALERT further strengthens the anonymity protection of source and destination by hiding the data initiator/receiver among a number of data initiators/ receivers. It has the “notify and go” mechanism for source anonymity, and uses local broadcasting for destination anonymity. In addition, ALERT has an efficient solution to counter intersection attacks. ALERT’s ability to fight against timing attacks is also analyzed. Experiment results show that ALERT can offer high anonymity protection at a low cost when compared to other anonymity algorithms. It can also achieve comparable routing efficiency to the base-line GPSR algorithm.

IV. PROPOSED ACTIVE ROUTING PROTOCOLS

A. Prism: Privacy Friendly Routing In Suspicious Manets

PRISM is an anonymous location-based on-demand routing protocol based on three main building blocks: (1) the well-known AODV routing protocol, (2) any secure group signature scheme, and (3) location information. PRISM uses a location-centric, instead of an identity-centric, communication paradigm. Therefore, it does not assume any knowledge of long-term node identifiers or public keys. (2) PRISM requires neither pre-distributed pairwise shared secrets nor on-line servers of any kind.

PRISM is designed with the following features in mind:
• The source authenticates the destination and vice versa. Node authentication means that the node is genuine and can be later identified in the event of misbehavior or disputes.
• Intermediate nodes do not learn current location of the source or the exact current location of the destination(s).
• Intermediate nodes are not authenticated. Route length (hop count) is not verified. Albeit, it can be lower-bounded using time, assuming no wormhole attacks.
• After route discovery, all communication between source and destination is encrypted and authenticated using a one-time (session-specific) secret key.

• The TTP (group manager) can later learn claimed locations of all nodes that engage in direct communication, i.e., serve as either sources or destinations. The TTP is thus capable of identifying suspicious or malicious behavior by nodes that generate too many route discoveries or move along implausible trajectories (i.e., lie about their location).
This is enabled by having all nodes record all route requests and route replies they process (as source, destination or intermediate nodes) and later off-load the accumulated information to the TTP.

B. Ao2p: Ad-Hoc On Demand Position Based Privacy Routing Protocol

Privacy is needed in ad hoc networks. An ad hoc on-demand position-based private routing algorithm, called AO2P, is proposed for communication anonymity. Only the position of the destination is exposed in the network for route discovery. To discover routes with the limited routing information, a receiver contention scheme is designed for determining the next hop. Pseudo identifiers are used for data packet delivery after a route is established. Real identities (IDs) for the source nodes, the destination nodes, and the forwarding nodes in the end-to-end connections are kept private. Anonymity for a destination relies on the difficulty of matching a geographic position to a real node ID. This can be enforced by the use of secure position service systems. Node mobility enhances destination anonymity by making the match of a node ID with a position momentary. To further improve destination privacy, R-AO2P is proposed. In this protocol, the position of a reference point, instead of the position of the destination, is used for route discovery.

C. Anodr: Anonymous On Demand Routing With Untraceable Routes For Mobile Ad Hoc Networks

ANODR, an anonymous on-demand routing protocol for mobile ad hoc networks deployed in hostile environments, addressing two close-related unlinkability problems, namely route anonymity and location privacy.

Based on a route pseudonymity approach, ANODR prevents strong adversaries, such as node intruders and omnipresent eavesdroppers, from exposing local wireless transmitters' identities and tracing ad hoc network packet flows. Moreover, ANODR also demonstrates that untraceable data forwarding without encrypted routing header can be efficiently realized. The design of ANODR is based on "broadcast with trapdoor information", a novel network security concept with hybrid features merged from both network concept "broadcast" and security concept "trapdoor information". This network security concept can be applied to multicast communication as well.

D. D-Anodr: Discount Anonymous On Demand Routing Protocol For Manets.

Discount ANODR – for anonymous on demand routing in mobile ad hoc networks. This provide peer-to-peer privacy of both payload and control messages using a cryptographically lightweight protocol relying solely on symmetric cryptography for its operation. As a result, achieve substantially lower computation and communication complexity in comparison with functionally related proposals, at the cost of only a minor reduction of privacy guarantees. Effectively, however, the achieved reduction of the burden borne by the user devices is believed to enable the actual deployment of a privacy preserving technique of this type; thus, it argue enhance privacy guarantees (in comparison to the status quo) as opposed to degrading them. This proposal achieves source anonymity and routing privacy. As long as less than half of the nodes close to or on a given route are compromised, an adversary will be unable to trace a route. The overhead analysis indicates approach increases the route discovery time over DSR for a typical application by less than an estimated four percent, making our protocol particularly suitable to use in ad hoc networks with high mobility

IV. CONCLUSION

This paper presents a number of anonymous routing protocols for MANET, which are broadly categorized as proactive and reactive. Proactive routing protocols tend to provide lower latency than that of the on-demand protocols, because they try to maintain routes to all the nodes in the network all the time. But the drawback for such protocols is the excessive routing overhead transmitted, which is periodic in nature without much consideration for the network mobility or load. On the other hand, though reactive protocols discover routes only when they are needed, they may still generate a huge amount of traffic when the network changes frequently. Depending on the amount of network traffic and number of flows, the routing protocols could be chosen. When there is congestion in the network due to heavy traffic, in general case, a reactive protocol is preferable. Sometimes the size of the network might be a major considerable point.

Network mobility is another factor that can degrade the performance of certain protocols. When the network is relatively static, proactive routing protocols can be used, as storing the topology information in such case is more efficient. On the other hand, as the mobility of nodes in the network increases, reactive protocols perform better. Overall, the answer to the debating point might be that the mobility and traffic pattern of the network must play the key role for choosing an appropriate routing strategy for a particular network. It is quite natural that one particular solution cannot be applied for all sorts of situations and, even if applied, might not be optimal in all cases. Often it is more appropriate to apply a hybrid protocol rather than a strictly proactive or reactive protocol as hybrid protocols often possess the advantages.

ACKNOWLEDGMENT

For comments and advice the author wishes to thank her tutor and guide R.Rajesh.

REFERENCES

[1] K.E. Defrawy and G. Tsudik, “ALARM: Anonymous Location- Aided Routing in Suspicious MANETs,” Proc. IEEE Int’l Conf. Network Protocols (ICNP), 2007.

[2] K.E. Defrawy and G. Tsudik, “PRISM: Privacy-Friendly Routing in Suspicious MANETs (and VANETs),” Proc. IEEE Int’l Conf. Network Protocols (ICNP), 2008.

[3] Y.-C. Hu, A. Perrig, and D.B. Johnson, “Ariadne: A Secure On- Demand Routing Protocol for Ad Hoc Networks,” Wireless Networks, vol. 11, pp. 21-38, 2005

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

[5] J. Kong, X. Hong, and M. Gerla, “ANODR: Anonymous on Demand Routing Protocol with Untraceable Routes for Mobile Ad-Hoc Networks,” Proc. ACM MobiHoc, pp. 291-302, 2003.

[6] L. Yang, M. Jakobsson, and S. Wetzel, “Discount Anonymous On Demand Routing for Mobile Ad Hoc Networks,” Proc. Securecomm and Workshops, 2006.

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

[8] T. Camp, J. Boleng, and V. Davies, “A Survey of Mobility Models for Ad Hoc Network Research,” Wireless Communications and Mobile Computing, vol. 2, pp. 483-502, 2002.

[9] X. Hong, M. Gerla, G. Pei, and C.C. Chiang, “A Group Mobility Model for Ad Hoc Wireless Networks,” Proc. Second ACM Int’l Workshop Modeling, Analysis and Simulation of Wireless and Mobile Systems (MSWiM), 1999.

[10] Debian Administration, http://www.debian-administration.org/ users/dkg/weblog/48, 2012.

[11] X. Wu, “DISPOSER: Distributed Secure Position Service in Mobile Ad Hoc Networks: Research Articles,” Wireless Comm. and Mobile Computing, vol. 6, pp. 357-373, 2006