Current Survey of Routing Protocols in MANETS

V. Deepalakshmi#1, T. Muthuramalingam#2
M.TechII Year (CSE), S.J.Spaul Memorial College of Engineering and Technology, Pondicherry University, Puducherry.

Ms. R. Vijayalakshmi#2
Assistant Professor
S.J.S Paul Memorial College of Engineering and Technology, Pondicherry University, Puducherry.

Abstract

Several routing protocols have been proposed in recent years for possible deployment of Mobile Ad-hoc Networks (MANETs) in military, government and commercial applications. MANET uses location-centric paradigm rather than identity-centric paradigm that are used in most of the networks. Using this paradigm is well suit ed for privacy in hostile and suspicious mobile ad-hoc networks. For achieving privacy and security, various protocols are proposed. This paper presents a survey on various protocols that are used in mobile ad-hoc networks for achieving privacy and security under hostile and suspicious scenarios.

Index Terms- Ad-hoc networks, routing protocols, Security, location-based protocols

1. INTRODUCTION

MANETs or Mobile Ad-hoc Networks is a type of ad-hoc network self-organizing and independent infrastructures, which make them an ideal choice for uses such as communication and information sharing. Because of the openness and decentralization features of MANETs, it is usually not desirable to constrain the membership of the nodes in the network.

A MANET is an autonomous collection of mobile users that communicate over relatively bandwidth constrained wireless links. Since the nodes are mobile, the network topology may change rapidly and unpredictably over time. The network is decentralized, where all network activity including discovering the topology and delivering messages must be executed by the nodes themselves, i.e., routing functionality will be incorporated into mobile nodes.

MANETS are vulnerable to attacks than wired networks. Open medium, dynamically changing network topology, cooperative algorithms, lack of centralized monitoring and lack of clear line of defense are some of the main vulnerabilities faced in MANETS. The applications of MANETs are military exercises, disaster relief, and mine site operation etc. These applications may benefit from ad-hoc networking, but secure and
reliable communication is the primary and necessary requirement for these applications.

The primary concern is became security in order to provide a secure and protected communication between mobile nodes in an open hostile environment. The main unique characteristics of MANETS are open peer-to-peer network architecture, shared wireless medium, stringent resource constraints, and highly dynamic network topology unlike the wire line networks. These characteristics cause a number of challenges to security design. The challenges that are nontrivial make a case for building security solutions that is able to achieve both broad protection and desirable network performance. The aim of the survey is to discuss different aspects of security and privacy in MANET and also study about some of the protocols (e.g. comparative study of different routing protocol (AODV, DSR).

This paper focuses on the survey of different routing protocols and is given in the following sections. Section II presents the literature survey of different routing protocols and a comparison table and section III concludes with discussions.

2. LITERATURE SURVEY

2.1. Dynamic Source Routing Protocol (DSR)

One of the simplest and efficient routing protocols designed particularly for use in multi-hop wireless ad-hoc networks of mobile nodes is the Dynamic Source Routing protocol (DSR) [5]. This protocol DSR allows the network to be completely self-organizing and self-configuring, without the need for any existing network infrastructure or administration.

DSR protocol is consists of two mechanisms one is Route Discovery and the other is route maintenance. These two mechanisms work together to allow mobile nodes to discover and maintain source routes to arbitrary destination nodes in the ad-hoc network. By the use of source routing, it allows packet routing to be trivially loop-free. The DSR protocol avoids the need for up-to-date routing information in the intermediate nodes through which packets are forwarded. It allows nodes forwarding or overhearing packets to cache the routing information in them for their own future use.

The aspects of this protocol operate entirely on-demand. It allows the routing packet overhead of DSR to scale automatically. It scales only to that needed to react to changes in the routes currently in use. The Dynamic Source Routing protocol (DSR) provides excellent performance for routing in multi-hop wireless ad-hoc networks. DSR has very low routing overhead and is able to correctly deliver almost all originated data packets, even with continuous, rapid motion of all nodes in the network.

2.2. Destination-Sequenced Distance-Vector Routing (DSDV)

A Mobile ad-hoc network or MANET is the cooperative engagement of a collection of Mobile Hosts without the required intervention of any centralized Access Point [6]. A MANET’s basic design idea is to operate each Mobile Host as a specialized router. This router periodically advertises its view of the interconnection topology with other Mobile Hosts within the network. Using this idea a new sort of routing protocol is developed. So, the investigated modifications to the basic Bellman-Ford
Routing mechanisms, as specified by RIP are used for dynamic and self-starting network mechanism. This mechanism is required by users wishing to utilize ad-hoc networks. These modifications address to solve the problems of Bellman-Ford, related to the poor looping properties of such algorithms in the face of broken links and the resulting time dependent nature of the interconnection topology describing the links between the Mobile Hosts. It also describes the ways for which the basic network-layer routing can be modified to provide MAC-layer support for mobile ad-hoc networks.

For the most convenient and efficient operation, information should be included along with the routing tables. The information in the routing table includes a sequence number, as well as settling time data useful for damping out fluctuations in route table updates. The sequence numbers are generated by the destination computer in each route table entry, except for the cases when a link has been broken; the latter case is described by a cometric and a sequence number which cannot be correctly generated by any destination computer.

The cometric route entries have sequence numbers which are odd numbers, and sequence numbers generated by each destination computer is an even number. The sequence numbers chosen to represent 243 broken links will be superseded by real routes propagated from the newly located destination as soon as possible by the natural operation of the protocol. The newly propagating routes will necessarily use a sequence number greater than what was used for the broken link since the latter sequence number is chosen to be one more than the last valid route’s sequence number. This causes the real route data to quickly supersede temporary link outages when a mobile computer moves from one place to another.

2.3. Ad-hoc On Demand Distance Vector Routing (AODV)

A novel algorithm for the operation of ad-hoc networks is the Ad-hoc on Demand Distance Vector Routing (AODV) [2]. Each Mobile Host operates as a specialized router and routes are obtained as needed (i.e., on demand). The routes are obtained with little or no reliance on periodic advertisements routing algorithm is quite suitable for a dynamic self-starting network as required by users wishing to utilize ad-hoc networks.

AODV provides loop free routes even while repairing broken links. Because the protocol does not require global periodic routing advertisements the demand on the overall bandwidth available to the mobile nodes is substantially less than in those protocols that do necessitate such advertisements. Nevertheless we can still maintain most of the advantages of basic distance vector routing mechanisms. Within the limits imposed by worst case route establishment latency as determined by the network diameter AODV is an excellent choice for ad-hoc network establishment. It will be useful in applications for emergency services conferencing battlefield communications and community based networking. We look forward to further development of the protocol for quality of service intermediate route rebuilding and various interconnection topologies with fixed networks and the Internet.

2.4. ALARM

In many traditional mobile networks scenarios, nodes establish communication on the basis of
persistent public identities. However, in some hostile and suspicious MANET settings, node identities must not be exposed and node movements must be untraceable. Instead, nodes need to communicate on the basis of nothing more than their current locations. In this address some interesting issues arising in such MANETs by designing an anonymous routing framework (ALARM) [3]. It uses nodes’ current locations to construct a secure MANET map. Based on the current map, each node can decide which other nodes it wants to communicate with. ALARM takes advantage of some advanced cryptographic primitives to achieve node authentication, data integrity, anonymity and intractability (tracking-resistance). It also offers resistance to certain insider attacks.

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. We have shown through simulation that node privacy under this framework is preserved even if a portion of the nodes are stationary, or if the speed of movement is not very high.

2.5. Optimized Link State Protocol (OSLR)

Optimized Link State Protocol (OSLR) is a proactive routing protocol, so the routes are always immediately available when needed. OLSR [4] is an optimization version of a pure link state protocol. So the topological changes cause the flooding of the topological information to all available hosts in the network. To reduce the possible overhead in the network protocol uses Multipoint Relays (MPR). The idea of MPR is to reduce flooding of broadcasts by reducing the same broadcast in some regions in the network, more details about MPR can be found later in this chapter. Another reduce is to provide the shortest path. The reducing the time interval for the control messages transmission can bring more reactivity.

OSLR uses two kinds of the control messages: Hello and Topology Control (TC). Hello messages are used for finding the information about the link status and the host’s neighbor’s. With the Hello message the Multipoint Relay (MPR) Selector set is constructed which describes which neighbor’s has chosen this host to act as MPR and from this information the host can calculate its own set of the MPRs. The Hello messages are sent only one hop away but the TC messages are broadcasted throughout the entire network. TC messages are used for broadcasting information about own advertised neighbor’s which includes at least the MPR Selector list. There is also Multiple Interface Declaration (MID) messages which are used for informing other host that the announcing host can have multiple OLSR interface addresses.

The MID message is broadcasted throughout the entire network only by MPRs. There is also a “Host and Network Association” (HNA) message which provides the external routing information by giving the possibility for routing to the external addresses. The HNA message provides information about the network- and the net mask addresses, so that OLSR host can consider that the announcing host can act as a gateway to the announcing set of addresses. The HNA is considered as a generalized version of the TC message with only difference that the TC message can inform about
route cancelling while HNA message information is removed only after expiration time.

2.6. PRISM

PRISM is designed with the following features in mind: the source authenticates the destination and vice versa. Intermediate nodes do not learn current location of the source or the exact current location of the destinations [1].

In PRISM, intermediate nodes are not authenticated. 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 privacy achieved by PRISM is not restricted to a specific mobility pattern.

The basic operation of PRISM is similar to AODV. PRISM allows a source to specify a destination area and simultaneously discover multiple destination nodes in it.

The PRISM Protocol has three building blocks: (1) the well-known AODV routing protocol, (2) any secure group signature scheme (or one-time public key certificates), and (3) location information.

2.7. ALERT

Routing protocol (ALERT) [8] to provide high anonymity protection (for sources, destination, and route) with low cost is dynamically partitions the network field into zones and randomly chooses nodes in zones as intermediate relay nodes, which form a non-traceable anonymous route [8]. Specifically, in each routing step, a data sender or forwarder partitions the network field in order to separate itself and the destination into two zones.

It then randomly chooses a node in the other zone as the next relay node and uses the GPSR algorithm to send 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. The reason we use ZD rather than D is to avoid exposure of D. Zone position refers to the upper left and bottom-right coordinates of a zone.

A packet in ALERT includes the source and destination zones rather than their positions to provide anonymity protection to the source and the destination. In addition, ALERT has a strategy to hide the data initiator among a number of initiators to strengthen the anonymity protection of the source. ALERT is also resilient to intersection attacks and timing attacks.

Avoiding the exhibition of interaction between communication nodes is a way to counter timing attacks. In ALERT, the “notify and go” mechanism and the broadcasting in ZD both put the interaction between S-D into two sets of nodes to obfuscate intruders. More importantly, the routing path between a given S-D and the communication delay (i.e., time stamp) change constantly, which again keeps an intruder from identifying the S and D.
3. CONCLUSION

This paper surveys different protocols used in MANET for achieving security and privacy. Many protocols like DSR, ALARM, AODV, DSDV, OSLR, PRISM are discussed in which all the protocols are concentrated in increasing the throughput, reducing the traffic overhead, end to end delay and achieving security and privacy.

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 on 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. ALERT offers identity and location anonymity of the source and destination, as well as route anonymity. Unlike geographic routing which always takes the shortest path, ALERT makes the route between a S-D pair difficult to discover by randomly and dynamically selecting the relay nodes.

4. REFERENCES


