DESIGN OF SECURE ROUTING PROTOCOLS FOR MOBILE AD HOC NETWORKS

Suresh Kanchi
Ph.D Student, Department of Computer Science and Engineering,
School of Engineering, SSSUTMS, Sehore.

Lalbahadur Kethavath
Assistant Professor, Department of Computer Science and Engineering
Teegala Krishna Reddy Engineering College, Hyderabad

Dr. R. P. Singh
School of Engineering, SSSUTMS, Sehore

ABSTRACT

The characteristics of Mobile Ad hoc Network (MANET) allows to call it as self-governing system of nodes in mobility and such mobile nodes are connected by wireless links. The MANET comes under class of wireless networks, particularly under infrastructure-less category. In MANET, the node acts as a termination system, also as an intermediate node and packet being forwarded by such node popularly called as router. The MANET nodes are in mobility therefore they change their locations. The node are enough capable to organize within them in turn changes happen dynamically for the current topology in which the node are. The major concern with respect to MANET nodes is, forming an optimum level and ideally an efficient route between any two parties wish to participate in exchange packets. It is the principal worry of the protocols related to the routing mechanism in MANET.

Key words: authentication, security, encryption, proactive, reactive, on-demand, MANET, attacks, AODV, DSR.

http://www.iaeme.com/IJCET/issues.asp?JType=IJCET&VType=9&IType=5

1. INTRODUCTION

We are in the era of the information storage and retrieval in the context of exchanging messages among the node in the network. The information may intended for a single node or multiple node or broadcasting. In this context, the information is distributed across the nodes in distributed environment. The information needs to be provided a security from attacks. It is to ensure authentication, confidentiality, integrity and availability. The attacks may be in different layers and are identified and studied in research. An intruder or attacker observe
network traffic and come in between the source and destination and thus control the network traffic flow. Therefore specially routing protocols or algorithms are compulsory to attend such issues. A single protocol mechanism that fits for all networks and solution for all possible issues is not perfectly suitable.

The protocols have to be according to network characteristics such as network size, density, and frequency of mobility of nodes. In this context, still improvement is an ongoing process in terms of research on mobile ad hoc networks. The research process to result hopefully and design of better performance protocols and probably to attend challenges that come in time period.

The MANET characteristics pull into the major challenges to be handled without giving away that is related to its design. Therefore the robust and tough security solutions can only protect MANET from attacks related to the route between any pair of nodes. The cryptographic techniques can be used for countermeasure of the routing-attacks on MANET.

1.1. Security

The operations in MANET have to be protected from the unauthorized and maliciously intended to exploit and disrupt the network. The prevention methods on attacks, includes authentication, encryption and decryption, can be incorporated to use to provide protection by reducing the possibility of attacks.

The attack in routing intended to disrupt overall communication and in turn to effect the whole network. With this context, the security and related mechanism plays most important part to secure the network (MANET). The paper includes consolidating the security methods for mobile adhoc networks and related issues and challenges. However, security solution requires to follow the sequence prevention, detection and reaction for the same.

1.2. Intermediate Nodes

The mobile ad hoc routing protocols have requirement for security considerations. In this, the trust in all the participants to correctly forward routing and data traffic is the main assumption. This assumption can prove to be terrible for an ad hoc network that relies, by no choice, most of the time on intermediate nodes, keeping trust on it, for packet forwarding.

The attempt has been made to survey the possibilities of the solutions to address the problem associated with secure and strong routing in mobile ad hoc networks. In particular, the system which is not equipped to verify identity of node or user before allowing for access data on system is obviously vulnerable to unauthorized data manipulation.

The MANET is more prone to vulnerable, challenges to explore possible solutions for the same. It so happens because of key characteristics of mobile ad hoc networks.

2. KEY CHARACTERISTICS

The MANET characteristics pull into the major challenges to be handled without giving away that is related to its design. Therefore the robust and tough security solutions can only protect MANET from attacks related to the route between any pair of nodes. The proposed methods to counter the routing-attacks on MANET can include cryptographic techniques.

The attack in routing intended to disrupt overall communication and in turn to effect the whole network. With this context, the security and related mechanism plays most important part to secure the network (MANET). It includes consolidating the security methods for mobile adhoc networks and related issues and challenges.
The MANET are different category networks with context that, they are infrastructure-less, every computer are device in the network take part to act as router as well as end host, every node in the network, node are autonomous by nature, nodes in mobility low energy nodes and computing services.

i) No centralized management: Lack of centralized coordinator or server. The detection of attacks is difficult because of the absence of centralized monitoring of nodes. The most important is, nodes are highly dynamic and large scale ad-hoc network resulting to frequent change of topology.

ii). Single-hop and Multi-hop: The major issue in MANET is to provide secure and reliable communication in such changing environment. The packet from a particular source node has to reach intended destination node, most of the time, it may need to use intermediate node to deliver it to the intermediate or destination node. The packet reaches destination via intermediate nodes, such mechanism is multi-hop, for packet delivery.

iii). Scalability of the network: The mobility of nodes result in joining new nodes into the network or leaving nodes from the network which creates a challenge to the ad-hoc network to handle related issue even concerning to its security.

iv). Cooperativeness: The primary assumption of routing algorithm for MANETs usually is that nodes are cooperative and no malicious. The malicious and non-cooperative nodes can easily become and take part as an important routing agent obviously with an intention to disorder the network operation by violating the protocol specifications.

v). Dynamic topology: The mobility of nodes in ad hoc network obviously is a challenging issue which creates dynamic topology of nodes. It in turn leads to frequent change in the computed routes, therefore the algorithms for determining a route between source and destination nodes has to managed every time,

vi). Bandwidth constraint: The nodes are wi-fi enabled, therefore form a topology to start communicating and packet exchanging over existing and constrained bandwith.

vii). Limited battery power supply: The nodes of ad hoc network are in mobility, in the sense that they have to work by help of stand-alone battery power supply. There, the capacity of battery is limited, which in turn root for several problems. This forces a node in mobile ad-hoc network to behave selfish to save energy and so may not be interesting in reception, processing and retransmission of forward packets.

viii). Boundary-less: In mobile ad-hoc network, the boundary of nodes which form topology is not predefined. The nodes work in a mobility and travelling environment where they are allowed to enter and leave topology network. The moment, any node, possible opponent node also, comes in the radio range of a node then it will join in the network and will be able to communicate with other nodes.

This situation, gives rise to possible attacks include eavesdropping, impersonation, tempering, replay and denial of service etc.
3. ROUTING PROTOCOLS

The mobile ad hoc network is infrastructure-less category of network, therefore, there is a chance of prone for many issues and security attacks such as confidentiality, integrity and service availability. The confidentiality refers to an unauthorized access or interception of data. The traffic over a route can be observed by an unauthorized node, which can be analyzed by applying techniques to know the information exchanged among nodes. The integrity attack is kind of attack on data, which includes repudiation, modification, replaying, masquerading. The availability of data or service can be threatened by kind of threat called denial of Services.

The routing protocol in an ad hoc network can be effected by some kind of attacks, which are discussed in the following.

**Disclosing of location:** is an attack that targets at the privacy requirements of an ad hoc network. With the use of techniques for traffic analysis, or with approaches for penetrating and monitoring, an attacker attempts to discover the present location of a node in the network, or the structure or topology of the entire network.

**Black Hole:** a malicious node advertise itself that there exist a shortest route via it to the intended destination node. It provides false information as reply for the route request that it receives. Such replies can be used and fabricated to divert traffic in the route through the malicious node for eavesdropping. There is a chance to attract all traffic to it and drop the packets by denial of service.

**Replay Attack:** During replay attacks the intruder node captures the packets and later injects into the network routing, so its receiver may treat is as a correct request or packet and take actions as per the packet but are desired by the intruder.

**Quality of Service:** the dynamic changes in topology in adhoc network, providing the quality of service. The fast development in the field of mobile technology and real time applications like multimedia, voice, providing of quality of service in ad hoc networks is a necessary aspect to maintain best-effort of service.

**Routing Overhead:** The wireless adhoc networks nodes often change their location within network. There are cases where some false routes possibly generated in the routing table which leads to the avoidable routing overhead.

**Power Consumption:** For most of the light-weight mobile nodes, the functionality related to communication should be optimized for so that it complete the process with lower consumption. Ultimately, conservation of power and power-aware routing must be taken into consideration.

4. AD-HOC ROUTING PROTOCOLS

The route is the path by which source node reaches the destination node however there may be intermediate nodes between the source and the destination. The main goal of routing protocols is to discover an optimal pathway which possibly includes minimal number of intermediate nodes between source and destination. Ultimately, the route should be created such as, less overhead and reasonable bandwidth to use in order to transmit the message on expected time. The routing protocols are broadly categorized to static dynamic.

In case of static routing, the administrator specifies the route using manual process. Similarly, dynamic routing depends on the status of the network. The routing table is been maintained at each node in the network. It gets modified based on the changes occur in the network, like node(router) is removed or added from or to the network. Each router announces its presence by flooding the information packets in the network, therefore, with
this every router in the network will have knowledge about the newly added or removed router and its presence.

The ad-hoc routing protocols are classified based on the routing strategy as table driven or source initiated which include proactive, reactive and hybrid routing protocols, it is with respect to the routing topology adopted to use in MANET. The proactive routing protocols constantly maintain and update the routing tables about the status of the network topology and are typically table-driven. The other is reactive or on demand routing protocols, therefore source start route discovery process only when the source node has to transfer packets.

4.1. Proactive Routing Protocols
The protocols compute routing information even before it is needed and maintain in the routing tables. Therefore, the protocols are called as proactive routing protocols. A routing information is maintained by each node, route to each other node, in the network topology. The topology structure may change due to mobility of nodes in it, therefore the routing information kept in the table gets updated periodically. The protocols like DSDV, WRP, OLSR, FSR, FSLS have been categorized as table driven and proactive set of protocols.

**Dynamic destination sequenced distance vector (DSDV or DDSDV):**
Each table maintained with it, contains the list of all available destination, and it also stores the number hops required to each node to reach. These table are going to be updated periodically. That is the routing information updating is a periodic or event driven. If there is any significant change happened with any node and its routing information, then such updates are transmitted immediately.

The DSDV requires that each node in the network to advertise its routing table to its current neighboring nodes.

**Wireless Routing Protocols:**
Each destination node maintains four things: distance table, routing table, link cost table, message retransmission list (MRL). Each of these table maintain appropriate information that helps to calculate the route.

**Fisheye State Routing Protocol isl:**
The set of node are computed as per the reachability in n-number of hops from a center node. From center node what are the set of nodes that can reached in 1-hops, 2-hops, 3-hops and so on defines the scope of fisheye. The route from source node to destination node contains a node from each hop circle.
Similarly, the optimized link state routing protocol (OLSR), hierarchical state routing (HSR), zone based hierarchical link state (ZHLS), Landmark Ad hoc Routing (LANMAR) approach table driven routing computation.

4.2. Reactive Routing Protocols
The routes are created by the source node only on demand. This is the route discovery mechanism, maintain the route until route is needed. If it confirms that the route is no longer needed the it discards the route. It is a better approach in adhoc networks, because they are resource limited and node are in mobility. The protocols DSR, AODV, ABD, PAR

Ad hoc on demand distance vector routing protocol (AODV) is a reactive routing protocol for mobile ad hoc networks and other wireless ad-hoc networks. It attempts to discover the route from source to destination and is initiated by source node on demand. In AODV request for route, the route reply and route error are the control messages. When source node wants to establish route to the destination nodes, source node first route requests a control packets to their adjacent nodes. In this, keeps on doing so until it finds route to the exiting destination node.

Dynamic source routing (DSR) Protocol. The DSR is a reactive type of protocol, in this, the path from the source to destination is selected when required. The Source node initiates and floods the route request packets in to the network. The intermediate nodes upon receiving, which are having route to the destination, will respond with the route reply packets. When the source node starts broadcasting the route request packets, the header of the route request packet is empty. The header of the route request packet starts filling.

4.3. Hybrid Routing Protocol
These types of protocols make use of the strengths of both the previously discussed protocols by combining them together to obtain better results. In the initial stage routing is done with some proactively prospected routes and then formation serves the demand from additionally activated nodes through reactive flooding [4].

ZRP Hybrid Routing Protocol Zone Routing Protocol (ZRP) is a hybrid protocol which combines the advantages of both proactive and reactive schemes. The ZRP routing protocols consists of different modules such as: Intrazone routing protocol, Interzone routing protocols [4].

5. NODES BAHAVIOUR
The nodes in the MANETS have different behavior attitude. It is classifiable into two types: Unintentional, Intentional.

The behavior is not up to the expected and does not behave as it agreed for, it may happen unintentionally, intentionally. The unintentional misbehavior includes the reasons: due to failure of nodes, and badly failed nodes. The node may misbehave intentionally, which includes the reasons: nodes are selfish and nodes are malicious by nature.

5.1. Dealing with Misbehavior Nodes
The nodes in the MANET probably in the route from source node destination node, accept the packet and keep quite. It is supposed to forward to the next node in the route, but it does not do it. The some methods to deal with misbehaving nodes are as mentioned below.

- Watchdog
- Pathrater
The watchdog is a application which runs on every node and keeps track of behavior of node. Its working method is described below.

(i) The packet transmission is intended from source node S to destination node D as shown in above diagram.
(ii) The intermediate nodes between the node S to node D, are A, B, and C. All the packets reach D via A, B, C.
(iii) Every node in the network maintains a buffer which stores information about recently sent packets.
(iv) The node S send to node A, A sends to node B and B sends to node C.
(v) Then, the node A overhears the packet transmission from B to C, it is confirmation for node A before removing the packet from its buffer.
(vi) If packet remains in the buffer longer time, then increments a failure count for node responsible.
(vii) If failure count exceeds a threshold value then node is determined to be misbehaving node, the same will be notified by the source node.

The functionality of watchdog would as said above, to identify the malicious and misbehaving nodes in the MANETs. The disadvantages with watchdog include various reasons.

5.2. Ambiguous Collision
The acknowledgement from node B to node A of the packet may collide with next packet from node S to node A. The node A has to receive acknowledgement from node B and next packet from node S, which lead to ambiguous collision.

5.3. Receiver Collision
The packet from node B to node C may collide with the packet from node D to node C. The node C is the receiver node, where there is a possibility for collision, hence it is receiver collision.
Design of Secure Routing Protocols for Mobile Ad hoc Networks

5.4. Transmission Power
The nodes in the MANETS are in mobility and they use battery enabled power, which has limited storage of power or power backup. Therefore, the node involved in so many transmissions of packets of data as well as for acknowledgement may consume lot of battery power.

5.5. False Misbehavior
The node A reports to node S regarding transmission of the packet from node B to node C, which may be correct or wrong report. The node A may give false report by misbehaving, there is no any other way for node S, it has to believe node A.

5.6. Collision
The group of nodes in collision have sophisticated attack.

5.7. Partial Dropping
It is very difficult to identify the node which involve in partial dropping of the packet. The nodes which do not drop or discard packets always, sometime they forward packets and sometime they do not forward packet.

6. CONCLUSIONS
In this, all the types of attacks and solutions possibly suitable have been discussed. Similarly, the secure ad hoc routing protocols and some improvement possible over new protocols. Each and every protocol will have a separate set of operational requirements to provides protection against different attacks. The more on a security analysis is to be attempted by focusing on its applicability of solutions which are described. The future scope is to attempt more focus on attacks and possible routing protocols.
REFERENCES


