Chapter 1

Overview

1.1 Background

1.1.1 MANET

MANET (Mobile and Ad hoc NETworks) are networks formed by nodes that are mobile. They use wireless communication to speak among them and they do it in an ad hoc manner. In this kind of networks, routing protocols have to be different than from the ones used for fixed networks. In addition, nodes use the air to communicate, so a lot of nodes might hear what a node transmits and there are messages that are lost due to collisions. The concept of servers has to be modified: there is no guarantee that a node will be able to reach another node, so things like DNS servers, certification authorities (CAs) and other entities that are assumed to be found in fixed networks cannot exist.

Nowadays, routing in such scenario has been achieved. Nevertheless, if it has to be broadly used, it is necessary to be able to do it in a secure way. In a network where the existance of central servers cannot be expected, it is needed that nodes will be able to communicate without the risk of malicious nodes impersonating the entities they want to communicate with. In a network where everybody is anonymous, identity and trust need to be redefined.

1.1.2 AODV

Ad Hoc On-Demand Vector Routing (AODV) protocol [36] is a reactive routing protocol for ad hoc and mobile networks. That means that AODV does nothing until a node needs to transmit a packet to a node for which it does not know a route. In addition, it only maintains routes between nodes which need to communicate. Its routing messages do not contain information about the whole route path, but only about the source and the destination. Therefore, routing messages have a constant size, independently of the number of hops of the route. It uses destination sequence numbers to specify how fresh a route is (in relation to another), which is used to grant loop freedom.

In AODV, a node does route discovery by flooding the network with a 'Route Request' message (RREQ). Once it reaches a node that knows the requested route, it replies with a 'Route Reply' message (RREP) that travels back to the originator of the RREQ. After this, all the nodes of the discovered path have routes to both ends of the path.

In addition to these routing messages, 'Route Error' messages (RERR) are used to notify the other nodes that certain nodes are not anymore reachable due to a link breakage.

1.2 SAODV

The Secure Ad hoc On-Demand Distance Vector (SAODV) is an extension of the AODV routing protocol that can be used to protect the route discovery mechanism providing security features like integrity and authentication.

Two mechanisms are used to secure the AODV messages: digital signatures to authenticate the non-mutable fields of the messages, and hash chains to secure the hop count information (the only mutable information in the messages). For the non-mutable information, authentication is perform in an end-to-end manner, but the same kind of techniques cannot be applied to the mutable information.

The information relative to the hash chains and the signatures is transmitted with the AODV message as an extension message (let us refer to it as Signature Extension).

1.2.1 SAODV hash chains

SAODV uses hash chains to authenticate the hop count of RREQ and RREP messages in such a way that allows every node that receives the message (either an intermediate node or the final destination) to verify that the hop count has not been decremented by an attacker.

1.2.2 SAODV digital signatures

Digital signatures are used to protect the integrity of the non-mutable data in RREQ and RREP messages. That means that they sign everything but the Hop_Count of the AODV message and the Hash from the SAODV extension.

When a RREQ is received by the destination itself, it will reply with a RREP only if it fulfills the AODV's requirements to do so. This RREP will be sent with a RREP Signature Extension.

When a node receives a RREP, it first verifies the signature before creating or updating a route to that host. Only if the signature is verified, will it store the route with the signature of the RREP and the lifetime.

1.3 SAKM

Simple Ad hoc Key Management (SAKM) provides a key management system that makes it possible for each ad hoc node to obtain public keys from the other nodes of the network. Further, each ad hoc node is capable of securely verifying the association between the identity of a given ad hoc node and the public key of that node.

This is achieved by using statistically unique and cryptographically verifiable address.

1.3.1 Delayed Verification

Delayed verification allows to have route entries and route entry deletions in the routing table that are pending of verification. They will be verified whenever the node has spared processor time or before these entries should be used to forward data packages.

1.4 Short Cut Detection

When a routing protocol for MANET networks (mobile and ad hoc networks) does a route discovery, it does not discover the shortest route but the route through which the route request flood traveled faster. In addition, since nodes are moving, a route that was the shortest one at discovery time might stop being so in quite a short period of time. This causes, not only a much bigger end-to-end delay, but also more collisions and a faster power consumption.

In order to avoid all the performance loss due to these problems, nodes could periodically discover shortcuts to the active routes that can be used with any destination vector routing protocol. The same mechanism can be used also as a bidirectional route recovery mechanism.