Security Using Pre-Existing Routing for Mobile Ad hoc Networks

G.Pushpa, 2 K.Komali,

Assistant Professor

Department of computer science & engineering
Dadi institute of engineering and technology,Anakapalle

Abstract— The flexibility and mobility of Mobile Ad hoc Networks (MANETs) have made them increasing popular in a wide range of use cases. To protect these networks, security protocols have been developed to protect routing and application data. However, these protocols only protect routes or communication, not both. Both secure routing and communication security protocols must be implemented to provide full protection. To address these issues, a novel secure framework (SUPERMAN) is proposed. The framework is designed to allow existing network and routing protocols to perform their functions, whilst providing node authentication, access control, and communication security mechanisms. This paper presents a novel security framework for MANETs, SUPERMAN.

Index Terms—access control, authentication, communication system security, mobile ad hoc networks

1 INTRODUCTION

MOBILE autonomous networked systems have seen increased usage by the military and commercial sectors for tasks deemed too monotonous or hazardous for humans. An example of an autonomous networked system is the Unmanned Aerial Vehicle (UAV). These can be small-scale, networked platforms. This topology generation service is offered by a variety of Mobile Ad hoc Network (MANET) routing protocols.

MANETs are dynamic, self-configuring, and infrastructure-less groups of mobile devices. They are usually created for a specific purpose. Each device within a MANET is known as a node and must take the role of a client and a router. Communication across the network is achieved by forwarding packets to a destination node; when a direct source-destination link is unavailable intermediate nodes are used as routers.

MANET communication is commonly wireless. Wireless communication can be trivially intercepted by any node in range of the transmitter. This can leave MANETs open to a range of attacks, such as the Sybil attack and route manipulation attacks that can compromise the integrity of the network.

Eavesdropped communication may equip attackers with the means to compromise the trustworthiness of a network. This is achieved by manipulating routing tables, injecting false route data or modifying routes. Man in the middle (MitM) attacks can be launched by manipulating routing data to pass traffic through malicious nodes. Secure routing protocols have been proposed to mitigate attacks against MANETs, but these do not extend protection to other data.

This paper proposes a novel security protocol, Security Using Pre-Existing Routing for Mobile Ad hoc Networks (SUPERMAN). The protocol is designed to address node authentication, network access control, and secure communication for MANETs using existing routing protocols.

SUPERMAN combines routing and communication security at the network layer. This contrasts with existing approaches, which provide only routing or communication security, requiring multiple protocols to protect the network.

2 RELATED WORK & PROBLEM ANALYSIS

MANET Routing

MANETs rely on intermediate nodes to route messages between distant nodes. Lacking infrastructure to administrate the manner in which packets are routed to their destinations, MANET routing protocols instead make use of routing tables on every node in the network, containing either full or partial topology information. Reactive protocols, such as Ad hoc On-demand Distance Vector (AODV), plan routes when messages need to be sent, polling nearby nodes in an attempt to find the shortest route to the destination node.

The basic versions of AODV and OLSR lack security mechanisms, allowing malicious nodes to interfere with the network in a variety of ways. The key contributing factor to this problem is an inability to distinguish legitimate nodes from malicious nodes.

Security Threats

The ITU-T Rec., through X.805, defines wireless end-to-end security in seven classifications, which are called dimensions. This system of classification allows for clear and convenient identification of security threats in a networks and potential solutions to those problems. The following security dimensions are identified:

- Access control is required to ensure that malicious nodes are kept out of the network.
- Authentication confirms the identity of communicating nodes.
Non-repudiation prevents nodes from broadcasting false information about previous transmissions, mitigating replay and related attacks.

Confidentiality prevents unauthorised nodes from deriving meaning from captured packet payloads.

Communication security ensures that information only flows between source and destination without being diverted or intercepted.

Integrity checking allows nodes to ensure packets received are in the same form they were sent, without modification or corruption.

Availability ensures that network assets are accessible. Periodic checking of node status or reports from a node to its neighbours are a common means of checking the availability of a resource.

Privacy prevents outside observers from deriving valuable information through passive observation.

MANET Routing Security

To tackle the problems that assumed legitimacy can cause, secure MANET routing protocols have been proposed. Secure Ad hoc On-demand Distance Vector (SAODV) and Secure Optimised Link State Routing (SOLSR) are secure implementations of AODV and OLSR respectively. SAODV secures the routing mechanism by including random numbers in Route Request packets (RREQs). If a routing packet arrives that re-uses an old packet number, that packet is invalid. Nodes observed sending re-played packets may be flagged as malicious. SAODV requires that at least two Secure RREQs (SRREQs) arrive at the destination node by different routes with identical random numbers to identify the source node.

Secure Communication

Internet Protocol Security (IPsec) is a secure communication framework extending confidentiality and authentication services. It is comprised of three key protocols: Authentication Headers (AH), Encapsulating Security Payloads (ESP) and Security Associations.

AH provides connectionless integrity and source authentication services. It does not provide route authentication, as IPsec does not account for the route taken to destination.

The Diffie-Hellman key generation algorithm is an example of a means of generating symmetric keys without the need to explicitly communicate any sensitive key information. Nodes exchange locally generated data using globally known primes and local secret data. The resulting variable (referred to as a key-share) is then communicated by both nodes, facilitating the calculation of a symmetric key that is identical at both ends, without the need to communicate sensitive data at any point. This allows the discreet and secure establishment of node-to-node confidentiality between specific node pairs.

3 The SUPERMAN Framework

SUPERMAN is a framework that operates at the network layer (layer 3) of the OSI model. It is designed to provide a fully secured communication framework for MANETs, without requiring modification of the routing protocol. Fig. 1 shows the flow of data from transport, through the network layer (including SUPERMAN) to the data link layer. The dashed boxes represent elements of SUPERMAN that process packets and provide confidentiality and integrity. SUPERMAN also provides node authentication.

Terminology

Key terms used when describing SUPERMAN include:

- Trusted Authority (TA)
- Certificate (CKp)
- Public Diffie-Hellman Key Share (DKSp)
- A static node responsible for node initialisation and processing of certificates; it is a prerequisite to SUPERMAN.
- A required per node and shared with other nodes to join the network
- A public value communicated authenticate with the network.

This key provides the basis for all broadcast communication security in a SUPERMAN network.
o between nodes
  - Private Diffie-Hellman Key Share (DKSpriv)
  - A private value, held by all nodes in the network and never communicated. Used as the shared secret for Diffie-Hellman key exchange
  - Payload data encrypted using an encryption scheme such as Aead
  - Symmetric key (SK)
  - SKe(s,d) is a security key used for encryption of end-to-end communication between a source and destination node, derived locally via KDF from the product of the DKSp and DKSpriv

SUPERMAN Framework Overview
Every SUPERMAN packet shares a common SUPERMAN packet header (SH), shown in Fig. 2. The data contained in the header can be broken down as follows:

- Packet Type denotes the function of the packet
- Timestamps provide uniqueness, allowing detection of re-played packets and providing a basis for non-repudiation of previously sent packets
- The protocol identifier indicates the layer 4 type of the encapsulated data. This would be the IP protocol number in an IP based network.

<table>
<thead>
<tr>
<th>Octets</th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
</tr>
</thead>
<tbody>
<tr>
<td>0 Type</td>
<td>Timestamp</td>
<td>Protocol Identifier</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Fig. 2. SUPERMAN Packet Header (SH) structure

Key Management
SUPERMAN relies on the dynamic generation of keys to provide secure communication.

The Diffie-Hellman key-exchange algorithm provides a means of generating symmetric keys dynamically and is used to generate the SK keys. SKb keys can simply be generated by means of random number generation or an equivalent secure key generation service.

Secure Node-to-Node Keys
SKe keys are used to secure end-to-end communication with other nodes, with one SKe key generated per node, for every other node also authenticated with the network. SKp keys are used for point-to-point security and generated in the same manner as SKe keys.

Storage
SUPERMAN stores keys in each node’s security table. The security table contains the security credentials of nodes with which the node has previously directly communicated, as shown in Table 1. This table has | entries, where | is the number of nodes that the node in question has directly communicated with. Table 1 shows an example of a security table belonging to node A.

4 CONCLUSION
SUPERMAN is a novel security framework that protects the network and communication in MANETs. The primary focus is to secure access to a virtually closed network (VCN) that allows expedient, reliable communication with confidentiality, integrity and authenticity services.

SUPERMAN addresses all eight security dimensions outlined in X.805. Thus, SUPERMAN can be said to implement a full suite of security services for autonomous MANETs. It fulfills more of the core services outlined in X.805 than IPsec, due to being network focused instead of end-to-end oriented.

IPsec is intended to provide a secure environment between two end-points regardless of route, and has been suggested by some researchers to be a viable candidate for MANET security. However, it does not extend protection to routing services. Nor does it provide low-cost security, requiring a lengthy set-up and teardown process, usually on a session basis.

Secure Point-to-Point Footers
Secure footers are appended to all communication packets sent between SUPERMAN nodes. SKbp and SKp(x) keys are used in broadcast and unicast integrity service provision respectively.

Certificate Exchange
A sequence diagram outlining the certificate exchange process is shown in Fig. 4.
SUPERMAN provides security to all data communicated over a MANET. It specifically targets the attributes of MANETs, it is not suitable for use in other types of network at this time. It sacrifices adaptability to a range of networks, to ensure that MANET communication is protected completely and efficiently. A single efficient method protects routing and application data, ensuring that the MANET provides reliable, confidential and trustworthy communication to all legitimate nodes.

Future work includes the implementation of SUPERMAN on a simple mobile node platform to allow experimental observation and profiling of its performance, the proposal of network bridging solutions capable of providing SUPERMAN services between two closed networks over an insecure intermediate network, and investigating the effects of variable network topology on SUPERMAN to better understand the role of the credential referral mechanism on overhead mitigation in SUPERMAN networks.

REFERENCES


