Security Using Pre-Existing Routing for Mobile Ad hoc Networks

[1]G.Pushpa, [2] K.Komali,

[12]*Assistant Professor*

[12]*Department of computer science & engineering*
[12]*Dadi institute of engineering and technology,Anakapale*

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 lauched 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 secu- rity at the network layer. This contrasts with existing ap- proaches, which provide only routing or communication security, requiring multiple protocols to protect the net- work.

2 Related Work & Problem Analysis

MANET Routing

MANETs rely on intermediate nodes to route messages be- tween distant nodes. Lacking infrastructure to adminis- trate the manner in which packets are routed to their des- tinations, MANET routing protocols instead make use of routing tables on every node in the network, containing ei- ther full or partial topology information. Reactive proto- cols, 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 con- tributing factor to this problem is an inability to distin- guish 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 dimenstions 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, mitigat- ing replay and related attacks.
- **Confidentiality** prevents unauthorised nodes from de- riving meaning from captured packet payloads.
- **Communication security** ensures that information only flows between source and destination without being di- verted or intercepted.
- **Integrity** checking allows nodes to ensure packets re- ceived 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 valu- able information through passive observation.

MANET Routing Security

To tackle the problems that assumed legitimacy can cause, secure MANET routing protocols have been proposed. Se- cure 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 ran- dom 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 destina- tion node by different routes with identical random num- bers to identify the source node.

Secure Communication

Internet Protocol Security (IPsec) is a secure commu- ni-cation framework extending confidentiality and authentication services. It is comprised of three key protocols:AuthenticationHeaders (AH), Encapsulating Secu- rity Payloads (ESP) and Security Associations .

AH provides connectionless integrity and source au- thentication services. It does not provide route authentica- tion, as IPsec does not account for the route taken to desti- nation.

The Diffie-Hellman key generation algorithm is an ex- ample of a means of generating symmetric keys without the need to explicitly communicate any sensitive key infor- mation. 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 com- municate sensitive data at any point. This allows the dis- creet and secure establishment of node-to-node confiden- tiality between specific node pairs .

3 The SUPERMAN Framework

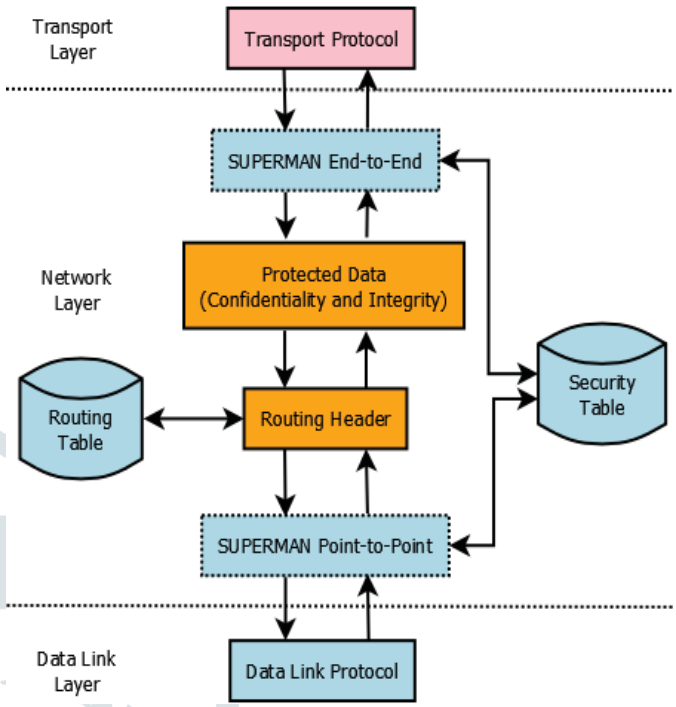


Fig. 1. Diagram illustrating the SUPERMAN confidentiality, integrity and authentication services for data packets

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 SUPER- MAN that process packets and provide confidentiality and integrity. SUPERMAN also provides node authentication.

Terminology

Key terms used when describing SUPERMAN include:

- Trusted Authority (TA)

o A static node responsible for node initialisation and pro- vision of certificates; it is a prerequisite to SUPER- MAN.

- Certificate (*CKp*)

o Required per node and shared with other nodes to join the network

- Public Diffie-Hellman Key Share (*DKSp*)

o A public value communicated thenticate with the network. This key provides the basis for all broadcast communication security in a SUPERMAN network.

- 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 Dif- fie-Hellman key exchange
  - Encrypted Payload (EP)
- 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 en- capsulated data. This would be the IP protocol number in an IP based network.

Octets	0	1	2	3	4
0	Type	Timestamp		Protocol Identifier	

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 gen- erated 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 communi- cated, as shown in Table 1. This table has *n* entries, where *n* is the number of nodes that the node in question has di- rectly communicated with. Table 1 shows an example of a security table belonging to node A.

Secure Point-to-Point Footers

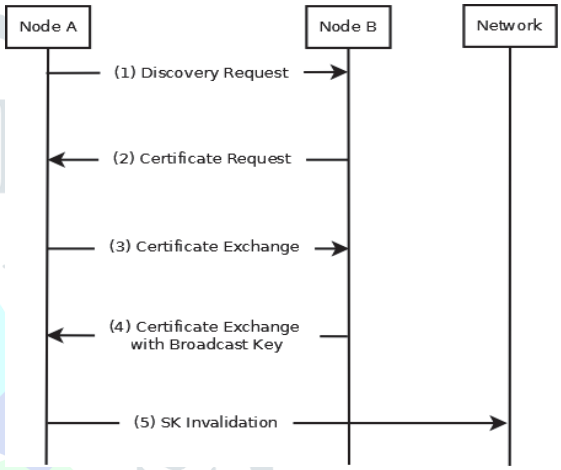
Secure footers are appended to all communication packets sent between SUPERMAN nodes. *SKbp* and *SKp(x)* keys are used in broadcast and unicast integrity service provi- sion respectively.

Secure Broadcast Keys

At initialisation of the network, the first node to be con- tacted about joining the network will generate a symmetric network key (*SKb*).

Certificate Exchange

A sequence diagram outlining the certificate exchange pro- cess is shown in Fig. 4.



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 imple- ment a full suite of security services for autonomous MA- NETs. It fulfils 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 be- tween 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.

SUPERMAN provides security to all data communi- cated over a MANET. It specifically targets the attributes of MANETs, it is not suitable for use in other types of net- work at this time. It sacrifices adaptability to a range of net- works, to ensure that MANET communication is protected completely and efficiently. A single efficient method pro- tects routing and application data, ensuring that the MA- NET provides reliable, confidential and trustworthy com- munication to all legitimate nodes.

Future work includes the implementation of SUPER- MAN on a simple mobile node platform to allow ex- perimental observation and profiling of its performance, the proposal of network bridging solutions capable of providing SUPERMAN services between two closed net- works over an insecure intermediate network, and investi- gating the effects of variable network topology on SUPER- MAN to better understand the role of the credential refer- ral mechanism on overhead mitigation in SUPERMAN networks.

REFERENCES

[1] P. S. Kiran, "Protocol architecture for mobile ad hoc networks," *2009 IEEE International Advance Computing Conference (IACC 2009)*, 2009.

[2] A. Chandra, "Ontology for manet security threats," *PROC. NCON, Krishnankoil, Tamil Nadu*, pp. 171–17, 2005.

[3] A. K. Rai, R. R. Tewari, and S. K. Upadhyay, "Differ- ent types of attacks on integrated manet-internet com- munication," *International Journal of Computer Science and Security*, vol. 4, no. 3, pp. 265–274, 2010.

[4] D. Smith, J. Wetherall, S. Woodhead, and A. Ad-ekunle, "A cluster-based approach to consensus based distributed task allocation," in *Parallel, Distributed and Network-Based Processing (PDP), 2014 22nd Euromicro International Conference on*. IEEE, 2014, pp. 428–431.

[5]

[6] D. Smith, J. Wetherall, S. Woodhead, and A. Ad-ekunle, "A cluster-based approach to consensus based distributed task allocation," in *Parallel, Distributed and Network-Based Processing (PDP), 2014 22nd Euromicro International Conference on*. IEEE, 2014, pp. 428–431.

[7] I. D. Chakeres and E. M. Belding-Royer, "Aodv rout- ing protocol implementation design," in *Distributed Computing Systems Workshops, 2004. Proceedings. 24th International Conference on*. IEEE, 2004, pp. 698–703.

[8] S. Bhattacharya and T. Basar, "Game-theoretic analy- sis of an aerial jamming attack on a uav communica- tion network," in *American Control Conference (ACC), 2010*. IEEE, 2010, pp. 818–823.

[9] S. Lu, L. Li, K.-Y. Lam, and L. Jia, "Saodv: a manet routing protocol that can withstand black hole attack," in *Computational Intelligence and Security, 2009. CIS'09. International Conference on*, vol. 2. IEEE, 2009, pp. 421– 425.

[10] S. Zhao, R. Kent, and A. Aggarwal, "A key manage- ment and secure routing integrated framework for mobile ad-hoc networks," *Ad Hoc Networks*, vol. 11, no. 3, pp. 1046–1061, 2013.