IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 23, Issue 3, Ser. I (May – June 2021), PP 12-16
www.iosrjournals.org

Secure Data Transfer Based On Key Exchange and Attack Prevention Protocol

Anna Denny
Computer science

Abstract: *The flexibility and mobility of Mobile Ad hoc Networks (MANETs)has become very popular because of their flexibility and mobility .To protect routing and application data security protocols has been developed. However, these protocols only protect routes or communication.Even though wireline and wifi networks are used to secure communication ,sometimes limited network resources of a MANET has became a heavy burden.This paper presents a narrative framework security for MANETs, SUPERMAN.The substructure is designed to allow existing routing protocols and network to perform their functions, whereas to contribute node authentication, communication security mechanism and access control.*

Index Terms: *communication system security, mobile ad hoc networks access control , authentication.*

Date of Submission: 04-05-2021 Date of Acceptance: 17-05-2021

I. Introduction

MANETs are dynamic, self-configuring, and infrastructure-less groups of mobile devices. They are usually created for a specific purpose.In MANET there is a device well known as a node and be obliged to take the role of a router and a client.Forwarding packets to the destination node helps for communication across the network .Intermediate nodes are usedas routers when a direct source destination link is unavailable. wireless communication can be superficially obstructed by any node in range of the transmitter.By this MANETs can have wide range of attacks. For example route manipulation and sybil attack. These attacks can compromise the integrity of the network [2]. MANET communication is commonly wireless. Autonomous systems require a significant amount of communication [4].To solve task planning problems without human intervention we need problem solving algorithms such as DTA (Distributed Task Allocation). This paper presents a narrative security protocol, Security Using Pre-Existing Routing for Mobile Ad hoc Networks (SUPERMAN).This protocol is conceived for MANETs using existing routing protocols such as secure communication , node authentication , network access control. Security using preexisting routing protocol using Mobile Adhoc Network [SUPERMAN] works in a network layer and combines routing and communication security.

II. Related Work & Problem Analysis

2.1 Security Threats

The ITU-T Rec., through X.805 [3], defines wireless endto-end security in seven classifications, which are called dimensions.This method of category allows for convenientnand clear rapport of security threats in networks and potential solution to those problems.The following security dimentions are rapported:

1.Access control is necessary to verify that malicious nodes are kept out of the network.

2. Authentication confirms the identity of communicating nodes.

3.Non repudiation debar nodes from transmitting wrong information about last transmission ,justifying replay and related attacks.

4.Clandestineness blocks unsanctioned nodes from deriving meaning from captured packet payload .

5.The information only flows between source and destination without diverted or intercepted.This process is ensured using communication security.

6.Without modification or corruption integrity checking allows nodes to ensure packets if they are received in the correct format as they sent.

7. Availability ensures that network assets are accessible.common way for checking the availability of a resource is by periodic checking of node status or reports from a node to its neighbours.

8.Outside observers can derive valuable information through passive observation and it is prevented by privacy .

2.2 MANET Routing

MANETs count on halfway nodes to route messages between distant nodes.

Non existent ground work to administrate the manner in which packets are conquerto their destinations .MANET routing protocol make use of routing tables on every node in the network ,hold partial topology information or either full.When messages have to be sent reactive protocols such as Adhoc On Demand Distance Vector (AODV)[5] plan the routes. To find the shortest route to the destination node , we will just give a try on polling nearby nodes.

2.3 Secure Communication

Securing routes is only one aspect of a full security solution. X.805 accentuate many security threats together with corruption ,data manipulation ,identity and theft [12]. There are three requirements to securing communication; authentication, confidentiality and integrity. X.509 sets the standard for certificate-based approaches to security [22].

To represent the identity of a given node and its releationship with trusted authority , the cerftificates provide a suite of data .Internet protocol security (IPsec) is a secure communication substructure extending authentication services, integrity and confidentiality. It is followed by three key protocol. .Security Associations (SA) , encapsulating security payloads (ESP)Authentication Headers(AH)[23].Authentication Head (AH) pludge connectionless data integrity and source authentication services . IPsec doesnot reckon for the route taken to a destination .it doesnot fork out route authentication.

2.4 MANET Routing

Routing security to intercept the problems that presume legitimacy can cause secure MANET routing complication .The secure implementation of AODVand OLSR are secure AdhocOn Demand Distance Vector (SAODV) and secure optimized link State Routing (SOLSR). Secure Adhoc On Demand Distance Vector includes random numbers in route request packets (RREQs) secures the routing mechanism[20].If a packet is invalid that means routing packet arrives and reuses the old packet number. The nodes were examined before sending replayed packets and it may be flagged as malicious .SAODV needs atleast two secure RREQs (SRREQs) to identify the source node and it arrives at the destination node by different routes with identical random numbers . SOLSR point to authorize detection of wormhole attack during its neighbours detection phase [14].To prevent malicious nodes from asserting themselves as neighbours, the node must be authenticated prior to establishing neighbor status. Verification of a source node's identity must be performed.Every node is persumed to have an asymmetric key pair . They are managed by coalition of nodes by using threshold cryptography.A system is required to manage , and to find if certificates are replaced in the field .For this distributed certificate Authority (CA) method is used.

III. The Superman Framework Overview

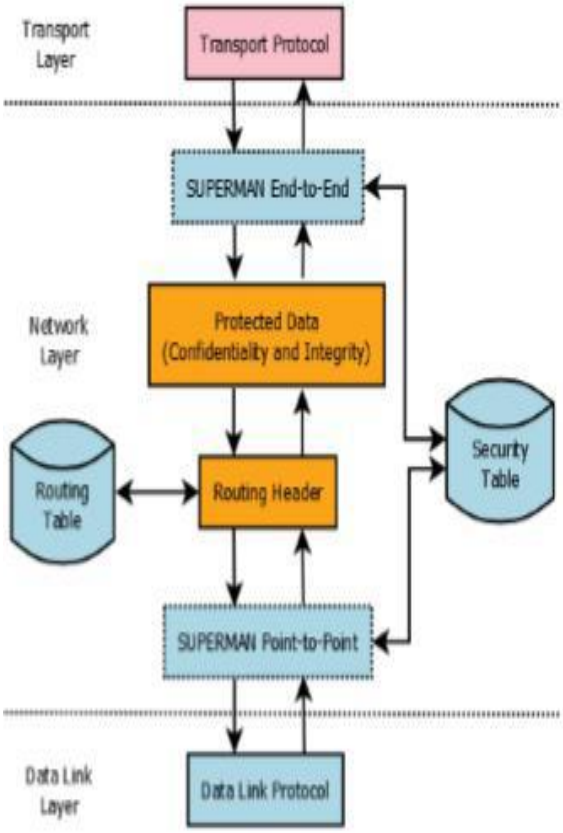
1. Packet type denotes the function of the packet

2.Timestamps furnish peculiarity recognizing detection of replayed packets and providing a basis for non repudiation of formerly sent packets . the protocol identifier indicates the layer 4type of the encapsulated data .

3.1 Terminology

Key terms used when describing SUPERMAN include:

- Trusted Authority (TA) - A static node responsible for node initialisation and provision of certificates; it is a prerequisite to SUPERMAN.
- Certificate (CKp) - Required per node and shared with other nodes to join the network
- Public Diffie-Hellman Key Share (DKSp) - A public value communicated 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
- Identifier (I) - A per node unique identifier, such as an IP address in an IP-based network
- Encrypted Payload (EP) - Payload data encrypted using an encryption scheme such as AEAD
- Tag (T) - A tag, appended as a footer to all SUPERMAN packets to provide point-to-point integrity services
- Symmetric key (SK) - SKe(s,d) is a security key used for encryption of end-toend communication between a source and destination node, derived locally via KDF from the product of the DKSp and DKSpriv o SKp(s,d) shared by two nodes; used to authenticate traffic as it moves along the network, derived locally via KDF from the product of the DKSp and DKSpriv
- Key Derivation Function (KDF(SK,func)) - A function used to provide multiple different keys from a common private source



3.2 Communication Security

Point-to-point Communication

When protected, data is propagated over multiple hops, it is authenticated at each hop. This is achieved using a hashing algorithm, such as HMAC. This is applied to the entire packet to provide point-to-point integrity.A tag is created using the shared SKp of the transmitting node and next hop ,which is idiosyncratic to the direct link .The Tag is restored at each intermediate hop, until the destination node is hold out. Thus, the authenticity of a route is maintained, as each node on the route must prove their authenticity to the next hop. This tag can also be used for integrity checking.

End-to-end Communication

End to End security come up with security services between source and destination nodes by wielding their shared SKe. Confidentiality and integrity come up with an appropriate cryptographic algorithm which can be used to give rise to an encrypted payload (EP).

3.3 Summary

SUPERMAN addresses the eight security dimensions detailed by X.805 come up with a closed MANET with end to end and point to point security.

- Access control is provided by SUPERMAN's network joining method.
- Authentication is provided by certificates, which allow the relationship between the node and TA to be confirmed
- Non-repudiation is provided by timestamps in each SUPERMAN packet header
- Confidentiality come up with end-to-end by payload encryption using AEAD
- Communication security is maintained by encrypting and performing source authentication end-to-end, and checking authenticity and integrity at every hop
- Integrity checking come up with by using a Tag for packet integrity.
- Availability is maintained at every nodes security table, which stores valid authentication credentials.
- Privacy come up with an end to end encryption ,with keys that are specific to the link between two nodes or a node and the network.

IV. Methodology And Results

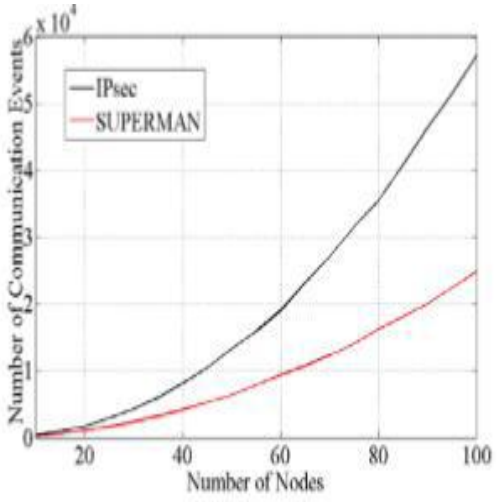
- Differentiation of security dimension coverage
- Number of communication events needed to secure communications between all nodes.
- Number of bytes needed to secure communications between all nodes.
- Elevated of securing communication needed for route generation.
- Elevated of securing commnunication needed by Consensus Based Bundle Algorithm (CBBA) AND Cluster Form CBBA (CF-CBBA)
- These costs constitute the additional data or packets , that are essential to dispense the security services, as the security is elevated..

4.1 Simulation Parameters

- MATLAB was chosen as simulation tool. Pre-existing CBBA simulation code has been used as a core for the DTA scenarios selected for these experiments, resulting in the network simulation being built alongside the DTA simulation
- It is supposed that every packets arrive intact unaccompanied bit error or loss,and the nodes are stationary during the initialization and association phases. The number of communication event constitute the total number of messages sent , anyhow it is based on packet size. It also furnish data regarding the length or routes , as each rely of a given will supplement the communication event count

MATLAB Simulation Parameters

Number of Nodes:	10 - 100
Routing Algorithm:	Dijkstrka [30] (shortest path)
Number of Iterations:	100
Simulation Area:	100m x 100m
Communication Range:	100m
Max Hop Count:	5
Random Seed:	11
Pseudo-random Number Generation Algorithm:	Mersenne Twister [31]
Key Share Size	128 and 256 bytes
Certificate Size	1013 and 1275 bytes



4.2 Initialisation cost of SUPERMAN and IPsec

- Method Comparison of the control overhead required by SUPERMAN and IPsec to initialise a secure network environment allows for the identification of the initialisation costs associated with each approach. These costs may materialize all round the lifetime of the network , but they are experienced only when nodes join the network. Two metrics are considered:
- The number of communication events.

- The number of bytes transmitted both metrics and they are measured until all nodes in a static set have joined the network.

4.3 Comparison of security overhead in routing

Method

The additional cost of secure routing is examined to determine the impact of SUPERMAN on a proactive and reactive MANET protocol.

Results

A single instance of network-wide routing is more demanding for AODV than OLSR (in terms of bytes required to complete the routing operation), but it must be noted that routes will be maintained under AODV until they time out. OLSR, however, will regenerate routes periodically. These results are therefore representative of the total cost for a network wide instance of routing, not the ongoing costs associated with routing on-demand or periodically.

V. Conclusion

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 fulfils more of the core services outlined in X.805 than IPsec, due to being network focused instead of endto-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.

SUPERMAN provides a VCN. It also furnishes a releativelylight weight encapsulation packet and variable length tag. 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

[1]. P. S. Kiran, "Protocol architecture for mobile ad hoc networks," 2009 IEEE International Advance Computing Conference (IACC 2009), 2009.
[2]. A. K. Rai , R. R. Tewari, and S. K. Upadhyay, "Different types of attacks on integrated manet-internet communication," International Journal of Computer Science and Security, vol. 4, no. 3, pp. 265–274, 2010.
[3]. H. Yang, H. Luo, F. Ye, S. Lu, and L. Zhang, "Security in mobile ad hoc networks: challenges and solutions," Wireless Communications, IEEE, vol. 11, no. 1, pp. 38– 47, 2004.
[4]. N. Garg and R. Mahapatra, "Manet security issues," IJCSNS, vol. 9, no. 8, p. 241, 2009.
[5]. 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.
[6]. A. Ghosh, R. Talpade, M. Elaoud, and M. Bereschinsky, "Securing ad-hoc networks using ipsec ," in Military Communications Conference, 2005. MILCOM 2005.IEEE. IEEE, 2005, pp. 2948–2953.
[7]. N. Doraswamy and D. Harkins, IPSec: the new security standard for the Internet, intranets, and virtual private networks. Prentice Hall Professional , 2003

Anna Denny. "Secure Data Transfer Based On Key Exchange and Attack Prevention Protocol." *IOSR Journal of Computer Engineering (IOSR-JCE)*, 23(3), 2021, pp. 12-16.