International Journal of Advance Research in Science and Engineering
Volume No.07, Special Issue No.06, March 2018
www.ijarse.com
IJARSE
ISSN: 2319-8354

Increasing Security in Virtually Closed Network using SUPERMAN Framework

K. Rahapriya[#1] , S. Saraswathi[#2], S. Rizviya Begam[#3], O. Shifana Affrin[#4],

Mrs. H. Prabavathi[*] M.Tech.(Ph.D),

[#]*UG Student, Department of Computer Science and Engineering*

A.V.C College of Engineering.

[*]Asst. Professor, Department of Computer Science and Engineering,

A.V.C College of Engineering.

ABSTRACT

The use of communication security protocols originally developed for wire line and Wi-Fi networks can even place an important burden on the restricted network resources of a MANET. The framework is meant to permit existing network and routing protocols to perform their functions, while providing node authentication, access management, and communication security mechanisms. Simulation results security SUPERMAN with IPSec, SAODV and SOLSR square measure provided to demonstrate the propose frameworks suitableness for wireless communication security. It gives secure transmission knowledge of information at the time the hackers hit the method received solely empty data. Eavesdropped communication might equip attackers with the means that to compromise the trustworthiness of a network. This can be achieved by manipulating routing tables injecting false route knowledge or modifying routes. Man in the Middle (MitM) attacks will be launched by manipulating routing knowledge to pass traffic through malicious nodes. Secure routing protocols are projected to mitigate attacks against MANETS, but these don't extend protection to alternative knowledge. This paper uses a completely unique security protocol, Security Using Pre-Existing Routing for Mobile Adhoc Networks (SUPERMAN). The protocol is meant to deal with node authentication, network access management,and secure communication for MANETs exploitation existing routing protocols. The aim is to transmit the data in secure path and the sender can identify the current location of the data. It also protect the data from any attackers can try to affect the network.

Keywords: *access management, authentication, communication security mechanism, mobile adhoc networks.*

I. INTRODUCTION

MANETs are dynamic, self-configuring, and infrastructure-less groups of mobile devices. MANET communication is commonly wireless. Wireless communication can be trivially intercepted by any node in range of the transmitter. Problem solving algorithms, such as Distributed Task Allocation (DTA), are required to solve task planning problems without human intervention. It secure path communication on one node to another node and data transfer will accuracy. This project proposes a novel security protocol, Security Using Pre-

Existing Routing for Mobile Ad hoc Networks (SUPERMAN). 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. 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. Autonomous systems require a significant amount of communication. As a result, these are vulnerable to packet loss and false messages; partial data will lead to sub-optimal or failed task assignments.

Mobile ad-hoc network is a combination of mobile nodes which forms a network which is temporary, without any requirement of fixed network infrastructure, where other commercial wireless technologies are based on towers and base stations. It is characterized by fast installation, low bandwidth, limited processing capability. In the nonexistence of proper security mechanism, mobile ad-hoc network is susceptible to many security attacks . An attacker node may act as an intermediate node which may threat to the data which is being transmitted. Ad-hoc on-demand distance Vector protocol, such as ad-hoc routing protocol is used to set routes between nodes and maintain the routes. The Ad-hoc on demand distance vector (AODV) routing protocol is on-demand routing protocol i.e. whenever route for a particular node is needed, routes are created. Each and every node in the network has a routing table which is maintained by AODV. It has one entry per destination and depending upon the sequence number routing information is updated that prevent routing loops. Main feature of AODV is to maintain the time based states in each and every node. Intrusion Detection System In networks, intrusion detection monitors activities of the network . First it the collects the activity information and analyzes whether there are any activities which violates the security rules. Since the mobile ad-hoc network exhibits many successful social applications such as Novel security (military Operations), Civil Sector, Medical diagnosis, Sensor Networks and ubiquitous computing the data need to be secured.

We design an Intrusion Detection System that detects intrusion in a MANET caused by malicious node launching different types of attacks with the help of threshold values, fuzzy logic and intuitionistic fuzzy, we tackle three types of routing attacks exhibits packet forwarding misbehaviour known as black hole attack, Gray hole attack towards source and Gray hole attack towards destination. We deal with different aspects such as the relative significance of symptoms, the varied symptom patterns of different attack stages. Here, the symptoms attack relationship constitutes one source of imprecision and uncertainty in the detecting process.

Portable self-ruling arranged frameworks have seen expanded use by the military and business areas for errands considered excessively dull or risky for people. A case of a self-sufficient organized framework is the Unmanned Aerial Vehicle (UAV). These can be little scale, arranged stages. Quadricopter swarms are an

essential case of such UAVs. Organized UAVs have especially requesting correspondence prerequisites, as information trade is indispensable for the on-going operation of the system. UAV swarms require consistent system control correspondence, bringing about regular course changes because of their versatility

This paper uses a novel security convention, Security Using Pre-Existing Routing for Mobile Ad hoc Networks (SUPERMAN). The convention is intended to address hub validation, organize get to control, and secure correspondence for MANETs utilizing existing directing conventions. SUPERMAN consolidates steering and correspondence security at the system layer. It protects both routing and communication at network layer.

II.RELATED WORKS

MANETs deem intermediate nodes to route messages between distant nodes. Lacking infrastructure to administrate the way within which packets square measure routed to their destinations, routing protocols instead build use of routing tables on each node within the network, containing either full or partial topology information.

Optimised Link State Routing (OLSR) takes a proactive approach, sporadically flooding the network to generate routing table entries that persist till future update. Both approaches area unit motion-tolerant and are implemented in UAV MANETs. Motion-tolerance and cooperative communication characteristics create these protocols ideal to be used in UAVs. The basic versions of AODV and OLSR lack security mechanisms, permitting malicious nodes to interfere with the network.

In a closed network, participation is restricted to authorised nodes, and communication is encrypted to prevent third-party comprehension of the contents of network communication. Authentication is required to allow new nodes to join and be seen as legitimate by existing network members.

The amount of time an individual UAV node may remain operational is limited by its battery life (energy), which may be shorter than the expected duration of the network's deployment. A replacement may be required if a node runs out of energy. Malicious nodes may masquerade as legitimate nodes, attempting to gain trusted status in the network by posing as a recently departed or newly arriving node.

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 Optimized 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.

The primary objective of SAODV and SOLSR is to prevent malicious nodes from gaining control of the topology generation mechanisms of the routing protocol, and to protect against black hole and wormhole attacks. Routing is secured and malicious node detection is employed in both cases.

Access control has been identified as a security dimension that might address the issue of implicit trust within a MANET. By closing the network to outsiders, the issue of assumed cooperation is circumvented. Closing the network requires a means of allowing nodes to join and leave the closed network .Authentication provides a means by which a node may be identified as trustworthy. By using a certificate to confirm that they share a trusted authority, two nodes may authenticate one-another based on their shared Trusted Authority (TA).

SUPERMAN, the protocol used in this paper, addresses the problem of unified MANET communication security. It implements a Virtual Closed Network architecture to protect both network and application data. And also sender can know the current location of the information. It provides empty content of information if any attackers hit the network.

III. NETWORK ACCESS CONTROL AND NODE AUTHENTICATION

A certificate-based method, such as X.509, is used to control access to the network . Every legitimate node in the network is provided with a certificate by the associated Trusted Authority (TA).

This node from different TAs to communicate securely within the same network. It establishing a hierarchical structure among TAs. This allows multiple controllers, each with their own TA, to share MANET resources if they share a hierarchy.

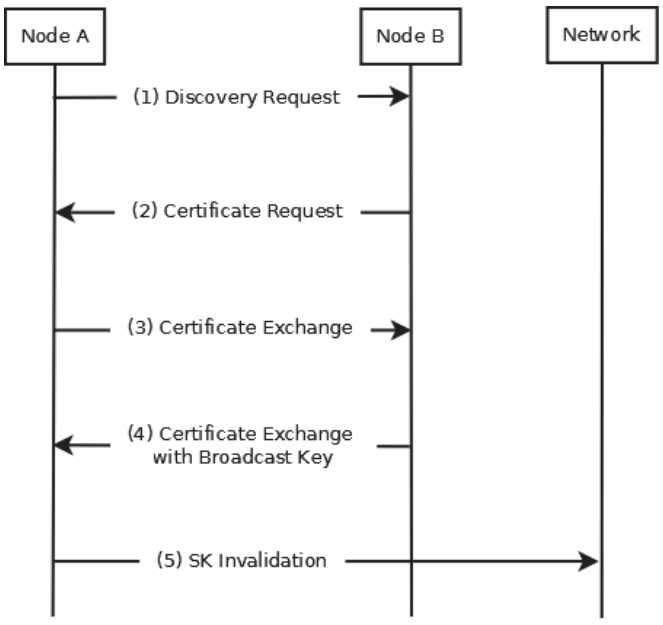

Fig 1.1 Sequence diagram to demonstrate the certificate exchange process

Terminologies used :

Key terms used when describing SUPERMAN include:

1. Trusted Authority (TA)

2. Certificate (CKp)
3. Public Diffie-Hellman Key Share (DKSp)
4. Private Diffie-Hellman Key Share (DKSpriv)
5. Encrypted Payload (EP)
6. Tag (T)
7. Symmetric key (SK)
8. Key Derivation Function (KDF)
9. Symmetric broadcast key (SKb)

Each node is provided with a certificate from a TA, in order for it to join SUPERMAN networks.

1. The joining node (*A*) seeks to join a network by periodically broadcasting Discovery Request (*DReq*) packets containing its *DKSp*. This continues until it receives a Certificate Request (*CReq*) from a networkable node (*B*).

2. Having received a *DReq* from node A, node B sends a *CReq* packet containing its *DKSp* to A. Both nodes perform Diffie-Hellman using the shared *DKSps* they now hold, to generate *SKe* and *SKp* keys which are used to encrypt and provide integrity to the rest of the access control process.

3. Upon receiving a *CReq* from B:

a. *A* sends its certificate in a Certificate Exchange (*CEx*) packet to *B*.

b. *B* checks the integrity and authenticity of the *CEx* packet, using the shared SKp.

c. *B* checks the certificate's authenticity against the TA hierarchy of its own certificate and the certificate contains the DKSp shared previously by A. If the certificate is deemed authentic *A* is added to *B's* security table.If the certificate fails this check, the *DKSp*, *SKe* and *SKp* credentials generated for node A by B are dropped and B and the process ends.

4. *B* responds to *A's CEx* with its own Certificate Exchange with Broadcast Key (CExB). *A* repeats steps *a* to *d* in 2. The CExB also provides A with the *SKb*, from which it derives *SKbe* and *SKbp* for broadcast communication, using the KDF. *B* and *A* both invalidate any prior security
associations they have with each other when receiving *DReq or CReq* packets with new information. This involves purging all previous information from their local security table entries for each other.

a. If B has not yet authenticated any other nodes, it will generate an *SKb*, prior to sending it to the joining node (A in this case), otherwise it will send the current *SKb* to the joining node

5. If *A* has a broadcast key, it transmits a Broadcast Key Exchange (*BEx*) packet containing the new key, secured with the original key before committing the new key to its security table.

6. *B* broadcasts an SK Invalidation (*SKI)* packet, invalidating any previous credentials *A* may have had with nodes within the network. This prevents the accumulation of expired security data on nodes that may be isolated from a previous invalidation event.

After authentication has been completed, both nodes will possess the following data:

 Each other's certificate

 The network share (*SKb*) to allow the derivation of broadcast keys via the function *KDF(SKb, type)* to allow secure broadcast communication

 Each other's Diffie-Hellman Key Share (*DKSp*), resulting in the calculation of *SK*, which is used in the function *KDF(SK, meta-data)* meta-data being a variable indicating whether the key is required for encryption or other security operations:

o *SKe* and *SKp* for end-to-end and point to-point secure communication

IV. SUPERMAN FRAMEWORK

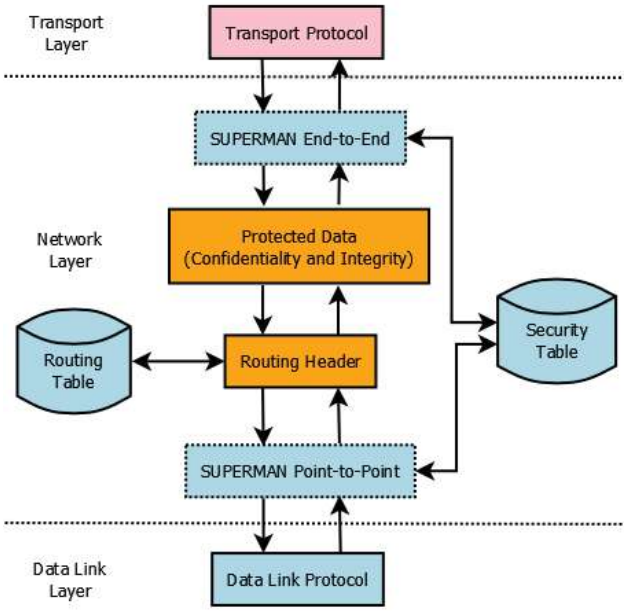

Fig 1.2 Illustrating the SUPERMAN confidentiality, integrity and authentication services for data packets

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

Every SUPERMAN packet shares a common 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 replayed packets and providing a basis for non-repudiation of previously sent packets

 The protocol identifier indicates the layer 4 type of the encapsulated data.

V. METHODOLOGY AND RESULTS

To analyze SUPERMAN, the following key areas were investigated:

- Comparison of security dimension coverage
- Number of communication events required to secure communications between all nodes
- Number of bytes required to secure communications between all nodes
- Overhead of securing communication required for route generation
- Overhead of securing communication required by Consensus

VI. CONCLUSION

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 provides security to all data communicated over a MANET. It sacrifices adaptability to a range of networks, to ensure that MANET communication is protected completely and efficiently. The original content of data transferred on particular node via MANET. 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.

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

[4].N. Garg and R. Mahapatra, "Manet security issues,"*IJCSNS*, vol. 9, no. 8, p. 241, 2009.

[5].A. R. McGee, U. Chandrashekhar, and S. H. Richman,"Using itu-t x. 805 for comprehensive network security assessment and planning," in *Telecommunications Network Strategy and Planning Symposium. NETWORKS 2004, 11th International*. IEEE, 2004, pp. 273–278

[6].M. G. Zapata, "Secure ad hoc on-demand distance vector routing," *ACM SIGMOBILE Mobile Computing and Communications Review*, vol. 6, no. 3, pp. 106–107,2002.

[7].D. Hurley-Smith, J. Wetherall, and A. Adekunle, "Virtual closed networks: A secure approach to autonomous mobile ad hoc networks," in *2015 10th International Conference for Internet Technology and Secured Transactions (ICITST)*. IEEE, 2015, pp. 391–398.

[8].M. Myers, R. Ankney, A. Malpani, S. Galperin, andC. Adams, "X. 509 internet public key infrastructureonline certificate status protocol-ocsp," RFC 2560,Tech. Rep., 1999.

[9].L. Harn, M. Mehta, and W.-J. Hsin, "Integrating diffiehellman key exchange into the digital signature algorithm (dsa)," *Communications Letters, IEEE*, vol.no. 3, pp. 198–200, 2004.

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