Secure Transmission by Using Mobile Ad hoc Networks

G. Arunkumar
Computer Science and Engineering
Anna University-
Thirukkuvalai.Nagapattinam

K. Balaji
Computer Science and Engineering
Anna University-
Thirukkuvalai,Nagapattinam

N. Chinnadhurai
Computer Science and Engineering
Anna University-
Thirukkuvalai,Nagapattinam

M. Rahulraja
Computer Science and Engineering
Anna University-Thirukkuvalai,Nagapattinam

D. Maria Manuel Vianny
Computer Science and Engineering
Anna University-Thirukkuvalai,Nagapattinam

Abstract:- The use of communication security protocols originally developed for wire line and WiFi networks can also place a heavy burden on the limited network resources of a MANET. 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.Simulation results comparing SUPERMAN with IPsec, SAODV and SOLSR are provided to demonstrate the proposed frameworks suitability for wireless communication security. It provide secure transmission of data at the time the hackers hit the process received only empty data. This paper presents a novel security framework for MANETs, SUPERMAN. To overcome the traffic issues, delay of transmission nodes and protect from attackers.The data transmission in secure path.

Index Terms*—*Network Access Control, Node Authentication, Terminology, Secured communication Framework, Communication Security.

*****

1. INTRODUCTION

Mobile autonomous networked systems have seen increased usage by the military and commercial sectors for tasks deemed too monotonous or hazardous forhumans. An example of an autonomous networked system is the Unmanned Aerial Vehicle(UAV). These can be small-scale, networked platforms. Quadricopter swarmsare a noteworthy example of such UAVs.

Networked.UAVs have particularly demanding communication requirements, as data exchange is vital for the on-going operation of the network. UAV swarms require regular network control communication, resulting in frequent route changes due to their mobility.

This topology generation service is offered by a variety of Mobile Ad hoc Network(MANET) routing protocols [1].

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 arouter.

Message across the network is completed byforwarding packets to a target node.

When a direct source-end link is unavailable intermediate nodes are used as routers.

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 solve task planning problems without human intervention.

It secure path communication on one node to two or more node and data transfer will accuracy.

This paper proposes a novel security protocol, Secure Transmission by using for Mobile Ad hoc Networks.

2. EXISTING SYSTEM

Multihoping algorithm used for the nodes transmission.

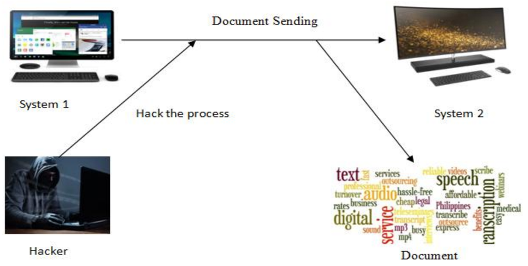
The data passes through between nodes the traffic will occur.

Due to traffic the time delay will occur.

The attackers can easily hack and view the data which content should be transfer.

The basic versions of AODV and OLSR lack securitymechanisms, allowing malicious nodes to interfere withthe network in a variety of ways [9], [10], [11].

SYSTEM ARCHITECHURE



DISADVANTAGE

- Traffic occur
- Time delay
- Easily hack the data

3. PROPOSED SYSTEM

SUPERMAN Algorithm used for the nodes transmission in this proposed system.

This Algorithm helps to transmit data via secured path as results traffic, delay time and attackers issues will be overcome.

The attacker hit the process we received only garbage content.

The original content of data transfer in secured path of communication on one node to two or more node.

The dashed boxes represent elements of SUPERMAN that process packets and provide confidentiality and integrity. SUPERMAN also provides node authentication.

3.1.TERMINOLOGY

Key terms used when describing SUPERMAN include:
Trusted Authority (TA)

Certificate (CKp)

Public Diffie-Hellman Key Share (DKSp)

PrivateDiffie-HellmanKeyShare(DKSpriv)

Encrypted Payload (EP)

Tag (T)

Symmetric key (SK)

Key Derivation Function (KDF)

Symmetric broadcast key (SKb)

3.2.SECUREDCOMMUNICATION FRAMEWORK

1. Key Management

2. Secure Node-to-Node Keys

3.Secure Point-to-Point Footers

4. Secure Broadcast Keys

5. Storage

3.3 COMMUNICATION SECURITY

1)End-to-end Communication

End-to-end security provides security services between source and destination nodes by using their shared SKe.

Authenticated Encryption with Associated Data (AEAD) is an example of such an algorithm. AEAD and related cryptographic algorithms provide confidentiality, authenticity and integrity services.

2) Point-to-point Communication

The data is propagated over multiple hops, it is authenticated at each hop. This is applied to the entire packet to provide point-to-point integrity. 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.

3) Broadcast

It uses the broadcast address for the network.

The packet is secured using the end-to-end and point-to-point methods. MANET routing protocols require broadcast capabilities. Both OLSR and AODV require broadcast communication for routes discovery.SUPERMAN provides broadcast communication security services to allow it to service the specific needs of MANET routing protocols.

3.4. NETWORK ACCESS CONTROL AND NODE AUTHENTICATION

A certificate-based method, such as X.509, is used to control access to the network [22].

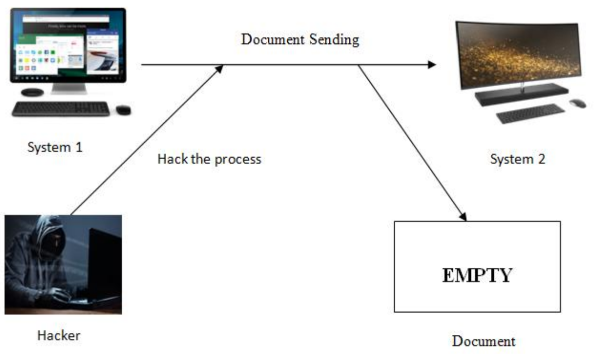
Every legitimate node in the network is provided with a certificate by the associated Trusted Authority (TA).

This allows nodes from different TAs to communicate securely within the same network, establishing a hierarchical structure among TAs.

This allows multiple controllers, each with their own TA, to share MANET resources if

they share a hierarchy.

SYSTEM ARCHITECTURE USING SUPERMAN ALGORITHM



ADVANTAGES

- To avoid time delay.
- To avoid traffic issues.
- Secure path identify.
- Data transfer secured.

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.

REFERENCE

[1] M. Myers, R. Ankney, A. Malpani, S. Galperin, and C. Adams, “X. 509 internet public key infrastructure online certificate status protocol-OCSP,” RFC 2560, Jun. 1999, Doi: 10.17487/ RFC2560.

[2] N. Doraswamy and D. Harkins, IPSec: The New Security Standard for the Internet, Intranets, and Virtual Private Networks. Upper Saddle River, NJ, USA: Prentice Hall Professional, 2003.

[3] A. Ghosh, R. Talpade, M. Elaoud, and M. Bereschinsky, “Securing ad-hoc networks using IPSEC,” in Proc. IEEE Mil. Commun. Conf., 2005, pp. 2948–2953.

[4] N. Ali, M. Basheeruddin, S. K. Moinuddin, and R. Lakkars, “Manipsec-ipsec in mobile ad-hoc networks,” in 3rd IEEE Int. Conf. Comput. Sci. Inf. Technol., 2010, vol. 1, pp. 635–639.

[5] E. Rescorla, “Diffie-hellman key agreement method,” RFC 2631, Jun. 1999, Doi: 10.17487/RFC2631.

[6] E. W. Dijkstra, “A note on two problems in connexion with graphs,” Numerische Mathematik, vol. 1, no. 1, pp. 269–271, 1959.