A SECURE APPROACH TO AUTONOMOUS MOBILE AD HOC NETWORKS

K.BALA MURUGAN,

P.NIJANDAN,

M.MALATHI,

Department Of Computer Science and Engineering

vks college of engineering and technology,tamilnadum

balacs97@gmail.com

malathim637@gmail.com

avatarnija@gmai.com

BY

A.POORANI, M.E

Assistant professor

Department Of Computer Science And Engineering

vks college of engineering and technology,tamilnadu

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. 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. 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. Simulation results comparing SUPERMAN with IPsec, SAODV and SOLSR are provided to demonstrate the proposed frameworks suitability for wireless communication security.

INTRODUCTION

MOBILE autonomous networked systems have seen increased usage by the military and commercial sectors for tasks deemed too monotonous or hazardous for humans.

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.

Communication across the network is achieved by forwarding packets to a destination node.

MANET communication is commonly wireless. Wireless communication can be trivially intercepted by any node in range of the transmitter. route manipulation attacks that can compromise the integrity of the 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.

Autonomous systems require a significant amount of communication. SUPERMAN is a novel security protocol, Security Using Pre-Existing Routing for Mobile Ad hoc Networks. The protocol is designed to address node authentication, network access control, and secure communication for MANETs using existing routing protocols.

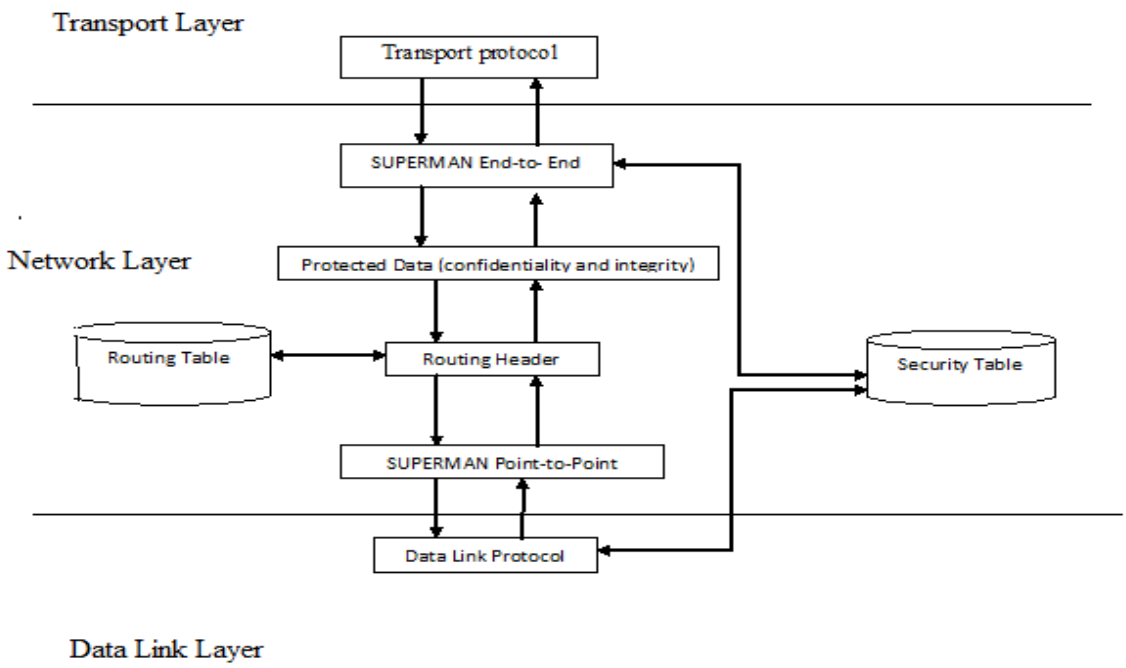
SUPERMAN combines routing and communication security at the network layer. This contrasts with existing approaches, which provide only routing or communication security, requiring multiple protocols to protect the network.

EXISTING SYSTEM:

In existing system, 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. The use of communication security protocols originally developed for wire line and Wi-Fi networks can also place a heavy burden on the limited network resources of a MANET.

PROPOSED SYSTEM:

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. The remainder of this paper is organized as follows: It analyses the problem in the context of previously published work. It introduces SUPERMAN, providing a technical discussion of the protocol. It outlines the characteristics chosen for modeling, and the results of simulating SUPERMAN compared against selected secure routing and data security protocols. It draws conclusions from the research findings.



ARCHITECTURE

Registration module:

registered user is a user of a website, program, or other system who has previously registered. Registered users normally provide some sort of credentials (such as a username or e-mail address, and a password) to the system in order to prove their identity: this is known as logging in. Systems intended for use by the general public often allow any user to register simply by selecting a register or sign up function and providing these credentials for the first time. Registered users may be granted privileges beyond those granted to unregistered users.

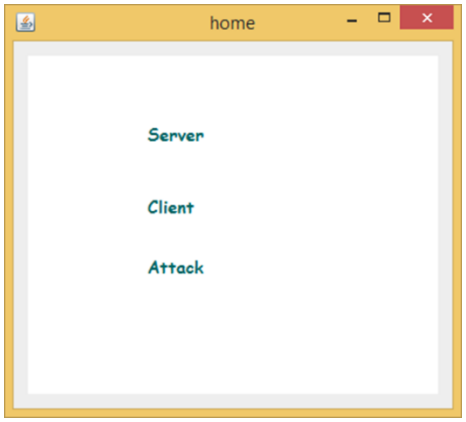
Login module:

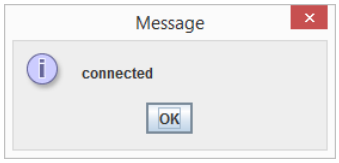
Logging in is usually used to enter a specific page, which trespassers cannot see. Once the user is logged in, the login token may be used to track what actions the user has taken while connected to the site.

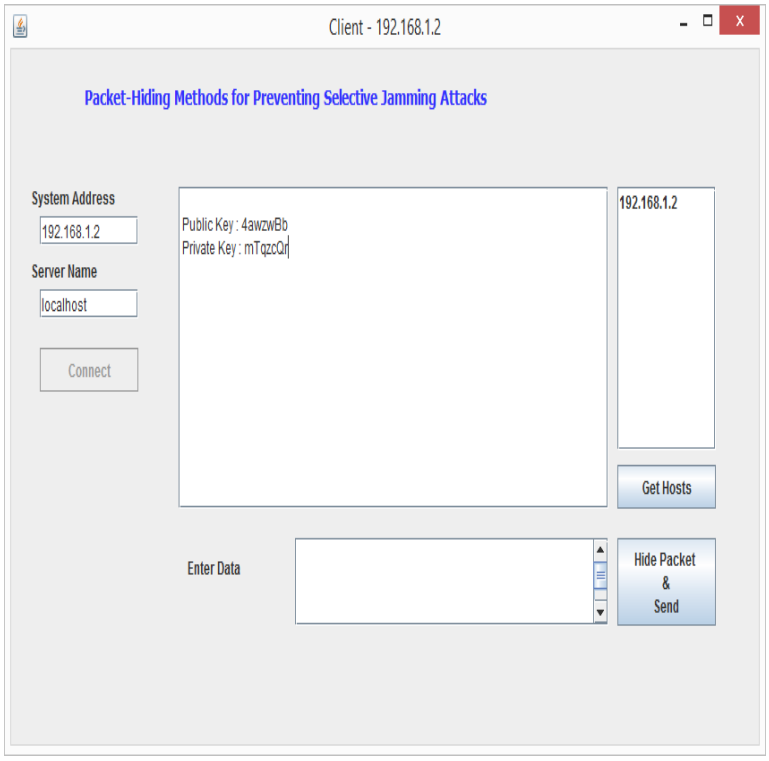
KEY GENERATION

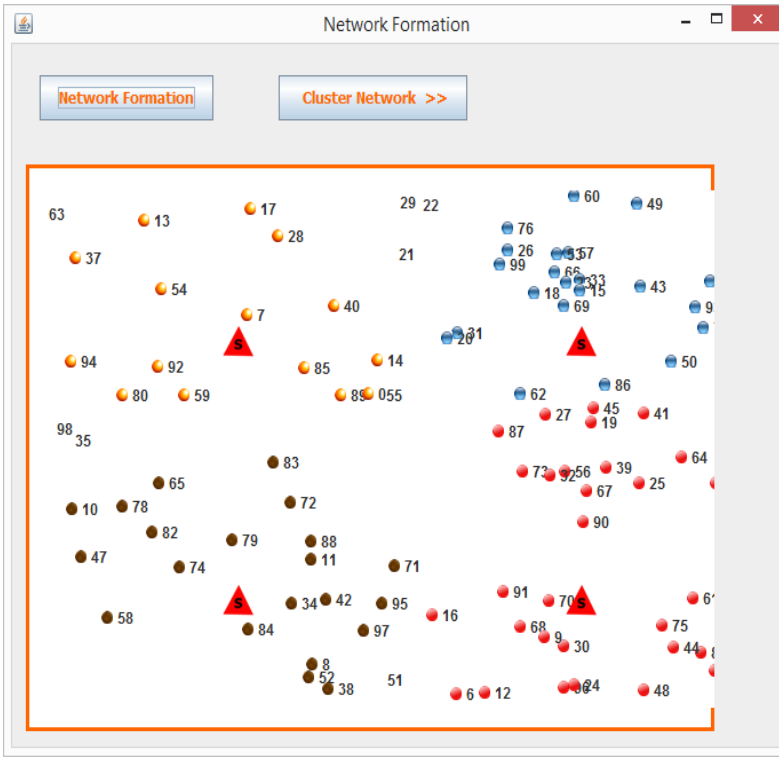
- Key generation is an important part where we have to generate both public key and private key. The sender will be encrypting the message with receiver's public key and the receiver will decrypt its private key. The key generated will be stored in a file.
- **CERTIFICATE AUTHENTICATION**
- The nodes(Sender and receiver) are verified for validity. If the nodes are valid then the packet will be transmitted. If the nodes are invalid then no packets are transmitted.
- **ATTACK DETECTION**
- The certificate authority is going to verify the RREP AND RREQ packets. If the sequence number are not matching then attack is detected otherwise no attack is detected
- Reach destination module
- At finally data reach original destination

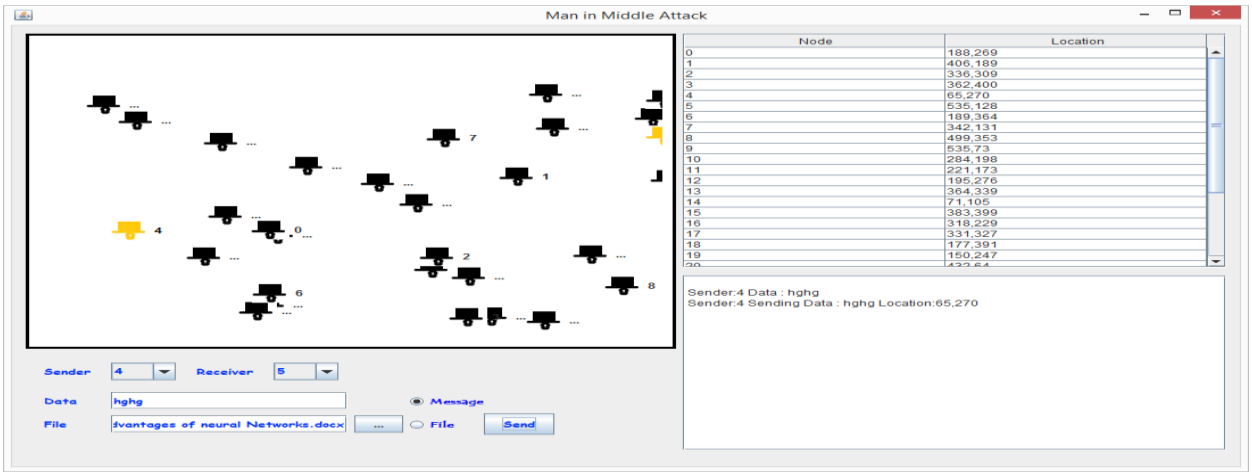
SCREEN SHOT






Client - 192.168.1.2
Packet-Hiding Methods for Preventing Selective Jamming Attacks
System Address
192.168.1.2
Server Name
localhost
Connect
Public Key : 4awzwBb
Private Key : mTqzcQr
192.168.1.2
Get Hosts
Enter Data
Hide Packet & Send


Network Formation
Network Formation
Cluster Network >>


Man in Middle Attack
Node
Location
0 188,269
1 406,189
2 336,309
3 362,400
4 65,270
5 535,128
6 189,364
7 342,131
8 499,353
9 535,73
10 284,198
11 221,173
12 195,276
13 364,339
14 71,105
15 383,399
16 318,229
17 331,327
18 177,391
19 150,247
Sender:4 Data : hghg
Sender:4 Sending Data : hghg Location:65,270
Sender
4
Receiver
5
Data
hghg
Message
File
dvantages of neural Networks.docx
File
Send

CONCLUSION

- The primary focus is to secure access to a virtual closed network (VCN) that allows expedient, reliable communication with confi-dentiality, integrity and authenticity services.

REFERENCES

[1] P. S. Kiran, "Protocol architecture for mobile ad hoc networks," in Proc. IEEE Int. Ad. Comput. Conf., 2009, pp. 2112–2117.

[2] A. Chandra, "Ontology for manet security threats," in Proc. 2nd Nat. Conf. Netw. Eng., 2005, pp. 171–117.

[3] A. K. Rai, R. R. Tewari, and S. K. Upadhyay, "Differen types of attacks on integrated manet-internet communication," Int. J. Comput. Sci. Secur., vol. 4, no. 3, pp. 265–274, 2010.

[4] D. Smith, J. Wetherall, S. Woodhead, and A. Adekunle, "A clusterbased approach to consensus based distributed task allocation," in Proc. 22nd Euromicro Int. Conf. Parallel, Distrib. Netw.-Based Process., 2014, pp. 428–431