ENHANCED SUPERMAN FRAMEWORK MODEL TO PREVENT SECURITY VULNERABILITES IN MANETS

[1]D.J.Samatha Naidu,[2]K.Asif Jelan
[1]Assistant professor, [2]MCA Student
[1]MCA Department,
[1, 2]Annamacharya PG college of Computer Studies, Rajampet ,Y.S.R kadapa, Andhra Pradesh,India

Abstract:MANET are dynamic, self-configuring and infrastructure-less groups of mobile devices. Each device with in a MANET is known as a node and must be 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 intermediates nodes are used as routers. MANET communication is commonly wireless can be trivially intercepted by any node in a range of transmitter. The flexibility and mobility of mobile ad-hoc networks (MANETS) have made open to a range of attacks, such as Sybil attack and route manipulation attacks that can be compromise the integrity of the networks. The key contributing factor to this is an inability to distinguish legitimate nodes from malicious nodes. The use of communication security protocols originally developed for wire lines and Wi-Fi networks can also place a heavy burden on the limited network resources of a MANET.

To address these issues, this work proposes a novel security protocol, enhanced security using Pre-Existing Routing for Mobile Ad hoc Networks (ESUPERMAN) .The protocols is designed to address node authentication, network access control, and secure communication for MANET using existing routing protocols. ESUPERMAN 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 primary focus is to secure access to a virtually closed network that allows expedient, reliable communication with confidentiality, integrity and authenticity services.

***IndexTerms*- Introduction,**

I. INTRODUCTION

Generally Mobile adhoc networks are specially designed and developed systems which may place major role on military and commercial sectors related applications, to protect monotonous and hazardous for humans. An example of an autonomous networked system is the Unmanned Aerial Vehicle (UAV). These can be small-scale, networked platforms. Quadricopter swarms are a noteworthy example of such UAV. Networked UAV have particularly demanding communication requirements, as data exchange is vital for the on-going operation of the network. This UAV swarms construct a regular network control to exchange data over network and network control routing communication changes their mobility in this areas.. This topology generation service is offered by a variety of Mobile Ad hoc Network (MANET) routing protocols .MANET 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.

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 (MIT) attacks can be launched by manipulating routing data to pass traffic through malicious nodes. Secure routing protocols have been proposed to mitigate attacks against MANET, but these do not extend protection to other data. Autonomous systems require a significant amount of communication. Problem solving algorithms, such as Distributed Task Allocation (DTA), are required to solve task planning problems without human intervention. As a result, these algorithms are vulnerable to packet Loss and false messages, partial data will lead to sub-optimal or failed task assignments.

In existing work (ESUPERMAN) Security Using Pre-Existing Routing for Mobile Ad hoc Networks was designed and developed for this MANET. The protocol is designed to address network node authentication, network access control mechanisms, and secure communication for adhoc networks using already work-in routing protocols. The Enhanced ESUPERMAN system interconnects all the routing and communication layers and provides security to the network layer and transport layer and session and application layer, where ESUPERMAN provides security up to network layer only. It supports all existing multipath scheduling protocols for MANETS. The remainder of this is organized as follows: analyses the problem in the context of previously published work. Outlines the characteristics chosen for modeling, and the results of simulating Enhanced ESUPERMAN compared against selected. Secure routing and data security protocols. Draws conclusions from research findings.

Purpose

This application purpose is providing the security for both routes and communications by using the pre-existing routing protocols for MANET.

Motivation of the work

The scope of the framework is designed to allow existing network and routing protocols to perform their functions. It is providing node authentication, access control, and communication security mechanisms. Presents a novel security framework for MANET, ESUPERMAN.

II Related Work

Existing Work

In existing system, Proactive and Reactive protocols are used such as Ad hoc On-demand Distance Vector (AODV), which allows the router to plan shortest path route from source to destination, when messages need to be sent, when attacker attacks the packets then polling nearby nodes in an attempt to find alternative shortest route to the destination node. The proactive approach supported by OLSR (optimized link state routing) which was designed specially to prevent flooding attacks over the network to generate routing table entries which helps for the next update. Both approaches are motion-tolerant and have been implemented in UAV MANETS. Motion-tolerance and co-operative communication characteristics make these protocols ideal for use in UAV.

Limitations

1 The basic versions of AODV and OLSR lack security mechanisms

2 Vulnerable to various attacks.

3 Inability to distinguish legitimate nodes from malicious nodes.

Proposed Work

Security Using Pre-Existing Routing for Mobile Ad hoc Networks (ESUPERMAN), the protocol is designed to address node authentication, network access control, and secure communication for MANET using existing routing protocols. . ESUPERMAN is a newly designed and developed framework , first establish a secure key establishment between source and destination parties to combine shortest path routing and provides communication security to OSI reference model layer such as network layer, transport layer, session layer and application layer. The previous work protocols supports only either routing or multiple path scheduling mechanisms that operates at the network layer (layer 3) of the OSI model. It provides data integrity and data confidentiality and authentication to nodes of a networks.

My contribution work as follows

1 Improve privacy of the network.

2 Increase data integrity.

3 Checks authenticity and integrity at each hop.

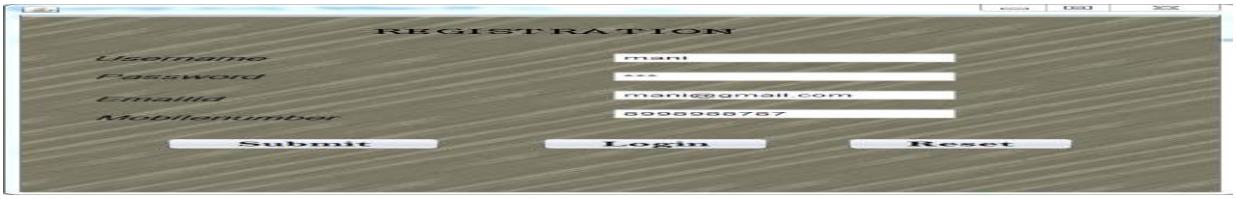
4 This protects the network and communication in MANETs.

5 Secure access to a virtually closed network (VCN).

6 It is providing the security against attackers.

IV.SIMULATION RESULTS AND COMPARATIVE ANALYSIS

The following software and hardware requirements are used to test the simulation results as follows, Processor core2duo, hard disk 160GB, RAM 1 GB, Operating System Windows 7, Coding language JAVA/J2EE, Tool Netbeans 7.2.1, Database MYSQL. When compare with other existing routing protocols security vulnerabilities are reduced. The following screens explain how the enhanced superman framework will work.



Screen 1: Home Page

Description: In the above fig shows the registration details about the user,contains the fields mentioned in that columns, after giving the details the user can be successfully registered.

Screen 2: Registration IP address

Description: After the giving the details in that fieldsthe user wants to register their account, the system asks the MAC Address.Then theMAC address is verified by the system after the verification the user registered to his account.

Screen 3: Registration Mack Address

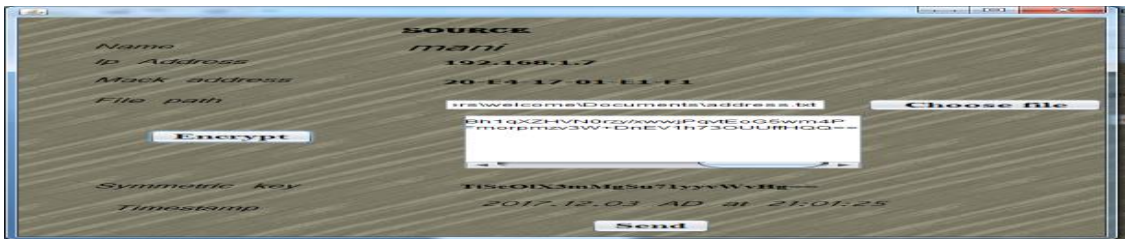
Description: After the giving the details in that fieldsthe user wants to register their account, the system asks the Mack Address.Then the mack address is verified by the system after the verification the user registered to his account.

Screen 4: Register Succesfully

Description: After entering the details the system verifies the details and the user registered a account ,then the system displays the register successful details.

Screen 5: Login

Description: After successful registration the user wants to login to their account the user wants to give their registration details after verifing the details the user login to their account.



Screen 6: Source Details

Description: After the user login to their account ,the user wants to send the file to the receiver ,the user need to choose the file for sending .

Screen 7: Data Send

Description: The receiver wants to receive the file from the user, thesystem needs to select the destination user name in the names column.Then the system find the shortest path to send file.

Screen 8: Network Security

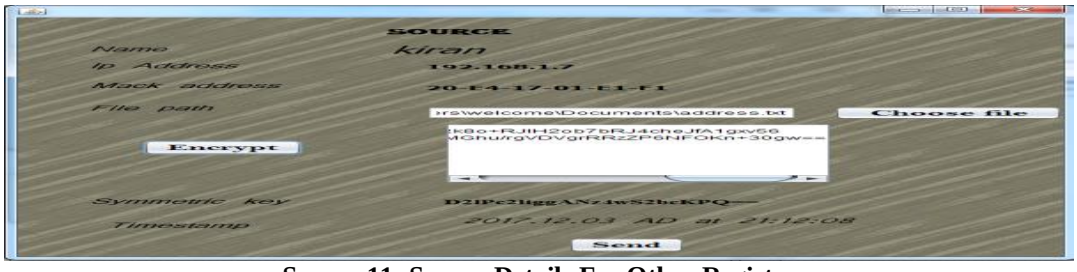
Description: After sending the data in the shortest path ,the user need to view the route path in which shortest path the data is received to the user .

Screen 9: Data Receive

Description: we can select the view route path .After the file can be reached to the source to destination,then the message will be display data will be received succesfully

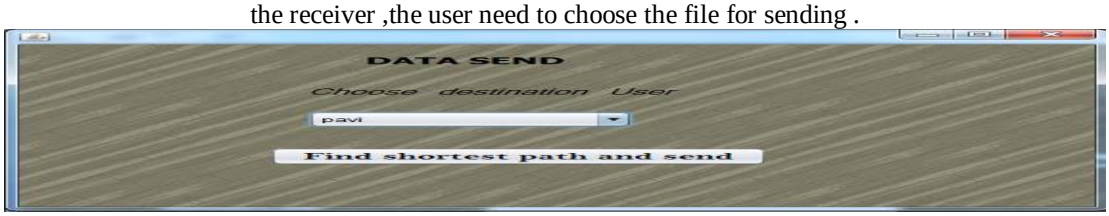
Screen 10: Destination Details

Description: Then select view route path.After will be display the destination page ,then we can select view data.



Screen 11: Source Details For Other Register

Description: In the above fig shows the source details. **:** After the user login to their account ,the user wants to send the file to the receiver ,the user need to choose the file for sending .

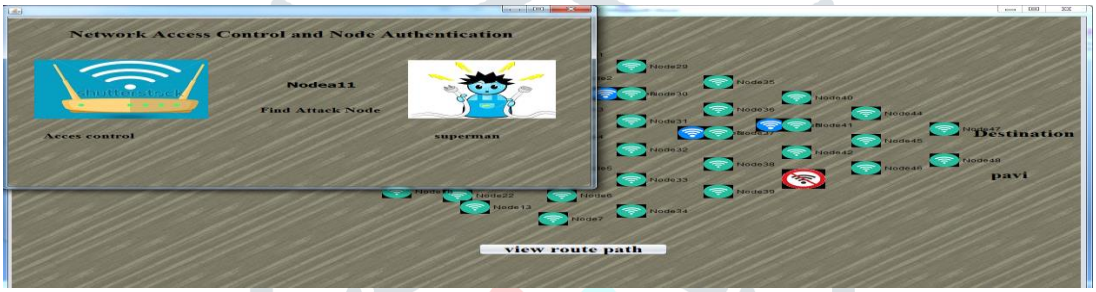


Screen 12: Data Send For Choose Another Destination user

Description : In the above fig shows the data send details. The receiver wants to receive the file from the user, thesystem needs to select the destination user name in the names column.Then the system find the shortest path to send file

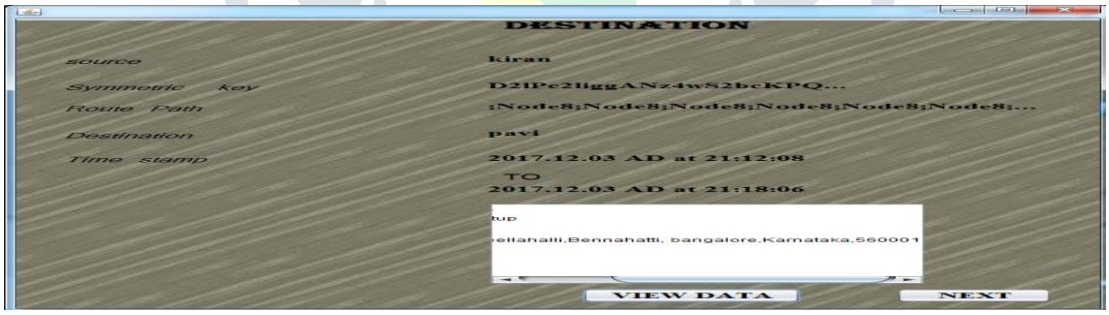
Screen 13: Attacker Select

Description: Then user can be selected the attack node ,after the packet will be selected ,then malicious data will be selected and click attack.



Screen 14: Network Access Control and Node Authentication

Description: After view route path will be selected ,then source to destination send the data can be third party will be received data ,the node number will be display.Then ESUPERMAN can be rectify the node after will be display the find attack node .

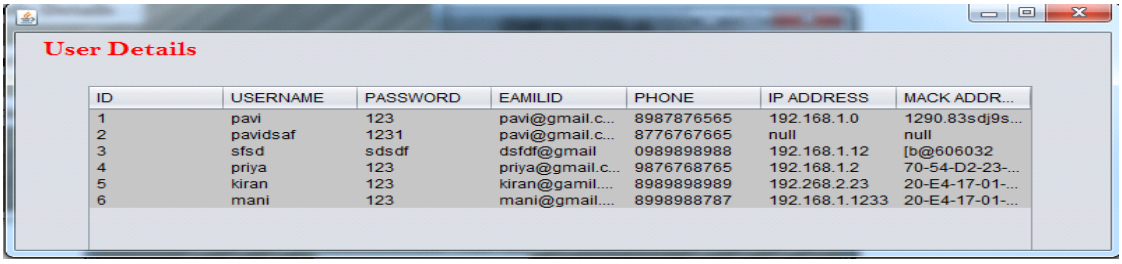


Screen 15: Attacker Destination Details

Description: Attacker destination the details source name and destination name,the route path will be display .After we click the view data.

Screen 16: Data Share Details

Description: The data share details will be display .After we select any one the information will be display

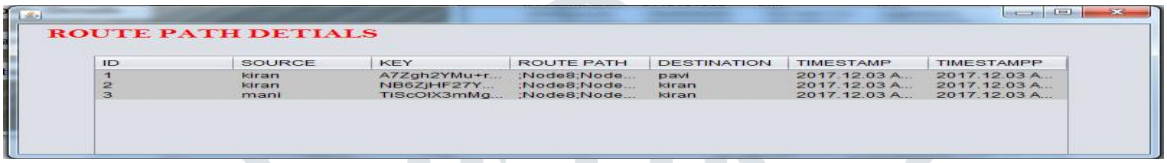


Screen 17: User Details

Description: In the above fig shows the user details.

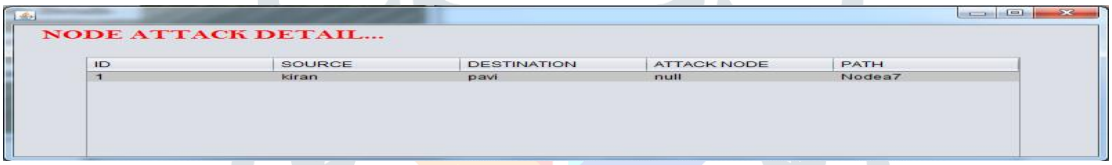
Screen 18: Node Details

Description: In the above fig shows the node details.



Screen 19: Route path Details

Description: In the above fig shows the route path details.



Screen 20: Node Attack Details

Description: In the above fig shows the node attack details.

Conclusion

ESUPERMAN is a novel security framework that protects the network and communication in MANETs. ESUPERMAN provides secure accessibility between multiple virtually closed networks that allows expedient, reliable communication with confidentiality, integrity and authenticity services. ESUPERMAN addresses all eight security dimensions outlined in X.805. Thus, ESUPERMAN can be said to implement full suite of security services for autonomous MANETs. It fulfills more of the core services outlined in X.805than IPsec, due to being network focused instead of end-to-end oriented.

Future Enhancements

Future work includes the ESUPERMAN services limited for inter domain routing protocols it may seems in future updated services may be provided for intra domain routing protocols, it may extend for web application services also.

II. ACKNOWLEDGMENT

We thankful to all the authors whose contribution works helps to solve our problems.

REFERENCES

[1] P. S. Kiran, "Protocol architecture for mobile ad hoc networks," 2009IEEE 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, "Different types of attacks on integrated manet-internet communication," International Journal of Computer Science and Security, vol. 4, no. 3, pp. 265–274, 2010.

[4] D. Smith, J. Wetherall, S. Woodhead, and A. Adekunle, "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] I. D. Chakeres and E. M. Belding-Royer, "Aodv routing protocol implementation design," in Distributed Computing Systems Workshops,2004. Proceedings.24th International Conference on. IEEE, 2004, pp. 698–703.

[6] 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.

[7] M. Hyland, B. E. Mullins, R. O. Baldwin, and M. A. Temple, "Simulation-based performance evaluation of mobile ad hoc routing protocols in a swarm of unmanned aerial vehicles," in Advanced Information Networking and Applications Workshops, 2007, AINAW'07. 21st International Conference on, vol. 2. IEEE, 2007, pp. 249–256.

[8] J. Pojda, A. Wolff, M. Sbeiti, and C. Wietfeld, "Performance analysis of mesh routing protocols for uav swarming applications," in Wireless Communication Systems (ISWCS), 2011 8th International Symposium on. IEEE, 2011, pp. 317–321.

[9] 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.

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

[11] 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.