IJNRD.ORG ISSN : 2456-4184
INTERNATIONAL JOURNAL OF NOVEL RESEARCH AND DEVELOPMENT (IJNRD) | IJNRD.ORG
An International Open Access, Peer-reviewed, Refereed Journal

# SUPERMAN: SECURITY USING PRE-EXISTING ROUTING FOR MOBILE AD HOC NETWORK

T.Dheena Thayalan, Student (Final year), CSE Department, PSN College of Engineering and Technology, Tirunelveli, Tamilnadu
Mr.A.Siva, Assistant Professor, CSE Department, PSN College of Engineering and Technology, Tirunelveli, 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 wired and wireless 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.

## I. INTRODUCTION

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

MANETs are dynamic, self-configuring, and infrastructure- less groups of mobile devices. They are usually created for a specific purpose. Each device within add 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. Wireless communication can be trivially intercepted by any node in range of the transmitter. 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.

## Mobile Computing

Mobile computing is the discipline for creating an information management platform, which is free from spatial and temporal constraints. The freedom from these constraints allows its users to access and process desired information from anywhere in the space. The state of the user, static or mobile does not affect the information management capability of the mobile platform. A user can continue to access and manipulate desired data while traveling on plane, in car, on ship, etc. Thus, the discipline creates an illusion that the desired data and sufficient processing power are available on the spot, where as in reality they may be located far away.

Fig.1..Structure of mobile computing

**OBJECTIVE**

**The objective is**

- To deploy the sensor nodes such that the network time is maximum.
- To schedule the sensor nodes so as to achieve the optimal network time.

**PROBLEM DEFINITION**

**Technical challenges in sensor network are,**

- Network discovery
- Control and Routing
- Collaborative signal and information processing
- Tasking and querying
- Security

# II. LITERATURE SURVEY

## INTRODUCTION

This chapter discusses the study and analysis conducted during this research on various conditions of Indian license plate images. A close glance on different license plate segmentation and their limitations are presented in this chapter. This process would enable the researchers to understand the research contributions in the area of license plate segmentation for Indian license plates.

## LICENSE PLATE SEGMENTATION

### 1) A cluster-based approach to consensus based distributed task allocation

**AUTHORS:** D. Smith, J. Wetherall

This paper presents a novel extension to the Consensus-Based Bundle Algorithm (CBBA), which we have named Cluster-Formed Consensus-Based Bundle Algorithm (CFCBBA). CF-CBBA is designed to reduce the amount of communication required to complete a distributed task allocation process, by partitioning the problem and processing it in parallel clusters. CF-CBBA has been shown, in comparison with baseline CBBA, to require less communication when allocating tasks. Three key aspects of task allocation have been investigated, (a) the time taken to allocate tasks, (b) the amount of communication necessary to satisfy the requirements of distributed task allocation algorithms such as CBBA, and (c) the efficiency with which a collection of tasks (a mission) is completed by a group of robots (a collective).

### 2) AODV routing protocol implementation design

**AUTHORS:** I. D. Chakeres and E. M. Belding-Royer

To date, the majority of ad hoc routing protocol research as been done using simulation only. One of the most motivating reasons to use simulation is the difficulty of creating a real implementation. In a simulator, the code is contained within a single logical component, which is clearly defined and accessible. On the other hand, creating an implementation requires use of a system with many components, including many that have little or no documentation. The implementation developer must understand not only the routing protocol, but all the system components and their complex interactions. Further, since ad hoc routing protocols are significantly different from traditional routing protocols, a new set of features must be introduced to support the routing protocol. In this paper we describe the event triggers required for AODV operation, the design possibilities and the decisions for our Ad hoc On-demand Distance Vector (AODV) routing protocol implementation, AODV-UCSB. This paper is meant to aid researchers in developing their own on-demand ad hoc routing protocols and assist users in determining the implementation design that best fits their needs.

# III. SYSTEM ANALYSIS

## EXISTING SYSTEM

- In existing system, Reactive protocols such as Ad hoc On-demand Distance Vector (AODV), plan routes when messages need to be sent, polling nearby nodes in an attempt to find the shortest route to the destination node.
- Another system i.e. Optimized Link State Routing (OLSR) takes a proactive approach, periodically flooding the network to generate routing table entries that persist until 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 UAVs.

## DISADVANTAGES OF EXISTING SYSTEM:

- The basic versions of AODV and OLSR lack security mechanisms
- Vulnerable to various attacks.
    - Inability to distinguish legitimate nodes from malicious nodes

## 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.
- 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 which process packets and provide confidentiality and integrity.
- SUPERMAN also provides node authentication.

## ADVANTAGES OF PROPOSED SYSTEM:

- Improve privacy of the network.
- Increase data integrity.
- Checks authenticity and integrity at each hop.

# IV. CONCLUSION

SUPERMAN is a novel security framework that protects the network and communication in MANETs. 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 addresses all eight security dimensions outlined in X.805. Thus, SUPERMAN can be said to implementation full suite of security services for autonomous MANETs. It fulfils more of the core services outlined in X.805than IP sec, due to being network focused instead of end-to-end oriented.

IP sec 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. Nor does it provide low-cost security, requiring a lengthy set-up and teardown process, usually on a session basis. Simulation has been undertaken and the results are reported and analyzed to determine the relative cost of security for SUPERMAN, compared against IP sec, SAODV and SOLSR where relevant.

SUPERMAN provides a VCN, in which the foundation block of security is provided by authenticating nodes with the network. This enables further benefits, such as the security association referral and network merging. It also provides a relatively light-weight encapsulation packet and variable length tag. Under both CBBA and CF-CBBA, the security overheads of SUPERMAN have been demonstrated to be lower than those of IPSec. Both DTA algorithms represent how a MANET can be made autonomous, by allowing problem solving without human intervention to occur on the network. Securing the communication required to facilitate this functionality is a critical consideration when providing a fully secured network. By providing lower cost security than existing alternatives, while providing security across all eight security dimensions, SUPERMAN proves it is a viable and competitive approach to securing the communication required by autonomous MANETs.

SUPERMAN has been shown to provide lower-cost security than SAODV and SOLSR for their respective routing protocols. By establishing a secure, closed network; one can assume a certain level of trust within that network. This reduces the need for costly secure routing behaviors designed to mitigate the effects of an un trusted environment(and un trusted nodes) on the routing process. By preventing the entry of potentially untrustworthy nodes to the network, and thus the routing process, a MANET may be protected from subversion of its routing services at a lower cost, as malicious nodes are barred from the process entirely. SUPERMAN provides security to all data communicated over a MANET. It specifically targets the attributes of MANETs, it is not suitable for use in other types of network at this time. It sacrifices adaptability to a range of networks, to ensure that MANET communication is protected completely and efficiently. A single efficient method protects routing and application data, ensuring that the MANET provides reliable, confidential and trustworthy communication to all legitimate nodes.

## V. FUTURE WORK

Future work includes the implementation of SUPERMAN on a simple mobile node platform to allow experimental observation and profiling of its performance, 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 to better understand the role of the credential referral mechanism on overhead mitigation in SUPERMAN networks.

## VI. REFERENCES

[1] P. S. Kiran, "Protocol architecture for mobile ad hoc networks," 2009 IEEE 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 Euro micro 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.24$^{th}$International Conference on. IEEE, 2004, pp. 698–703.

[6] T. Clausen, P. Jacquet, C. Adjih, A. Laouiti, P. Minet,P. Muhlethaler, A. Qayyum, L. Viennotet al., "Optimizedlink state routing protocol (olsr)," 2003.

[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] W. Ivancic, D. Stewart, D. Sullivan, and P. Finch, "An evaluation of protocols for UAV science applications,"2011.

[12] 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. NETWORKS2004, 11th International. IEEE, 2004, pp. 273–278.