IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 15, April 2026
Impact Factor: 8.2

Security Mechanisms in Mobile Adhoc Networks

Pawan Kumar Saini and Dr. Kelapati
Research Scholar, Research Guide, Department of Computer Science & Engineering
Shri Jagdishprasad Jhabarmal Tibrewala University, Jhunjhunu

Abstract: *Mobile Adhoc networks (MANETs) are accepted effortlessly worldwide due to their potential of bringing low cost mobile connectivity solutions to everyday communication problems. These networks have been widely applied in many commercial and military applications. Therefore, security of these networks has become imperative and vital challenge. The main goal of the thesis is to design a robust, efficient and accurate method for providing security in MANETs. In this regard, various security methods have been studied and efforts has been made to find out appropriate solution which can provide security in a given mobile adhoc networks. Although various security methods are available in literature, but all have their own advantages and disadvantages. Thus, the objective is to find more suitable method for MANETs application and evaluate it in terms of network throughput, accuracy, delay, energy and time required for detection of an attack in any given network.*

Keywords: MANET, Routing, Cognitive Radio (CR), Network Simulation, Wireless Ad-Hoc Network

I. INTRODUCTION

Mobile adhoc networks (MANETs) are wireless/infrastructure-less and resource constraint, having collection of nodes with high mobility feature. MANETs have acquired significant importance in today's mobile communication world subsequently it has acquired popularity in imperative applications such as military, rescue operations, tactical operations, environmental monitoring, conferences etc. The basic architecture of MANETs in shown in the figure 1.1 below. MANETs because of their mobility and infrastructure-less characteristic like are more vulnerable to attack as compare to conventional wired networks.

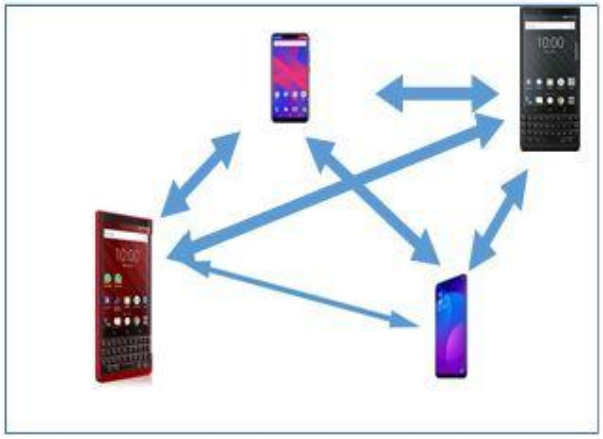

Figure1.1: Architecture of Mobile Adhoc networks

In last decade, Cognitive Radio (CR) paradigm which is another scheme of MANETs, has also arisen as an encouraging and innovative solution to evade complications of spectrum paucity and incompetence in spectrum usage by the users in a network. The classification of Adhoc Networks is depicted below in figure 1.2.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 15, April 2026
Impact Factor: 8.2

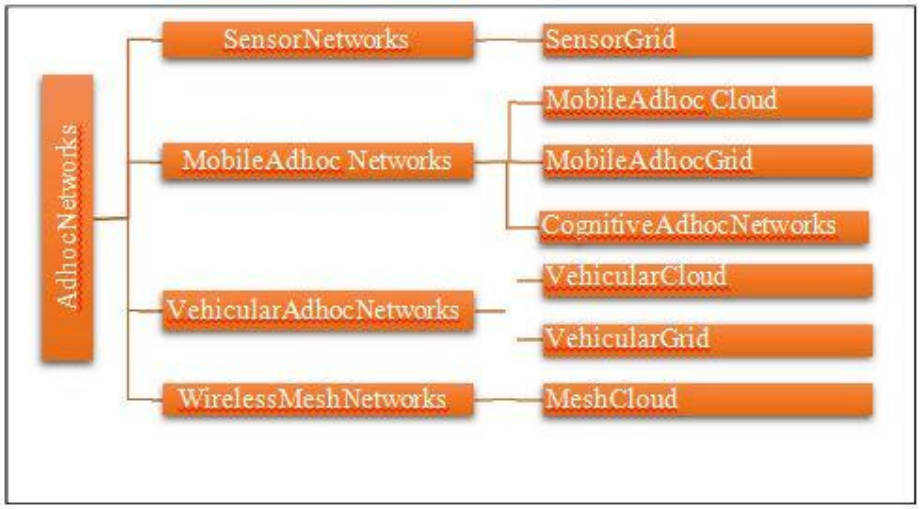

Figure 1.2: Classification of Adhoc networks

Considering the raised demand of access/controlling the devices on move by user, Mobile adhoc networks and its variant Cognitive Radio Adhoc Networks has become the most emergent technology, which motivates researcher to build efficient & stable secure system. To deduce an efficient method for obtaining robust security in the MANETs, initially, there is requirement to understand the challenges & issues which are discussed in following paragraph. Subsequently, deliberation on securing MANETs methods has been presented which are main objectives of this work.

II. TYPES OF AD HOC NETWORKS

According to range of the communication among the peer-to-peer networks, adhoc networks can be divided into following categories: -

Body Area Network : A Body Area Network (BAN) is formed by wearable computers whose units are distributed on a person's body (it includes, head-mounted display units, earphones, microphones, etc.). BAN offers communication between these units. The communication range of a BAN is thus same as that of a person's body range, that is, 1-2m.

Personal Area Network : Personal Area Network (PAN) is used to establish communication among mobile nodes carried by humans to other movable as well as stationary nodes. Therefore, a PAN corresponds to an environment around the person. The communication range of a PAN is up to 10 m.

Wireless Local Area Network : Wireless Local Area Network (WLAN) provides more flexibility as compared to wired LAN. Like wired LANs, the communication range of a WLAN is up to 100- 500 meters.

Wide Area ad hoc Network : Wide Area ad hoc Network is a class of wireless networks. In this, the different network nodes communicate with each other using multiple hops. There are several unresolved challenges (like addressing, location management, routing, security, etc.) faced by this network due to which they are not likely to become available for some time.

III. PROPERTIES OF MANETS

The most distinctive characteristic of MANETs is that they do not use any preestablished infrastructure. They form networks when mobile nodes come in range of each other. This type of network does not need any central administration and hence therefore there is no requirement of stationary devices such as bridges, routers, cables etc. The mobile nodes in MANETs forward data packets on behalf of other nodes which are not in the range of the destination node. The persistence and operations of MANETs depend on the forwarding behavior of the nodes making up the network. If nodes do not transmit packets on behalf of other network nodes, which means, if nodes do not

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 6, Issue 15, April 2026 Impact Factor: 8.2

participate in data routing process, network can be segmented and then the functionality of the network would be affected.

One another characteristic of MANETs is that they are autonomous. Autonomous means that, they generally provide and establish communication among the participating internal nodes and do not establish communication with external networks like LANs or internets. Though, some of the MANET nodes can be multi-homed having communication with different networks i.e. MANET and one or more external networks. These types of nodes are called gateway nodes that may exist in MANETs but it is not a common phenomenon. Additionally, Dynamic network topology is one another important characteristic of MANETs. The routing protocols employed in MANETs have to be able to adapt with this dynamic network topology feature.

IV. CHALLENGES & ISSUES IN MOBILE ADHOC NETWORKS

The main challenge of MANETs is to route packet with minimum overheads even when conditions are dynamic. Overhead is termed as use of channel bandwidth and battery power of mobile nodes for communication/processing procedure. Due to node mobility, and the dynamic characteristics of the radio channel, node connections in a route may become temporarily unavailable, which makes the route void. The overhead in discovering alternative routes arises besides additional packet delivery delay.

The other challenges of MANETs are listed below: -

i. Infrastructure less network
ii. Dynamic Changing topologies
iii. Physical layer Restrictions
    a. Controlled wireless range
    b. Packet drops in transmission
    c. Broadcast nature of the transmission
iv. Resource restrictions in mobile nodes
    a. Less battery life
    b. Restricted power/memory capacity
v. Network Security
vi.Unicast/Multicast Routing
vii. Route updates or Network Overhead
viii. Mobile-agent-based Routing
ix. Node moving speed
x. Quality of Service (QoS)
xi. Energy efficient or power aware routing
xii. Protected Routing techniques

V. PROBLEM STATEMENT

MANET is an emerging area of infrastructure-less networks formed by mobile nodes and confronts many routing challenges. These challenges are typically because of limited resources at the node and no central control. An adhoc environment is generally set up for temporary purposes, in circumstances of emergency or simply when there are no available resources for setting complex networks. MANETs therefore create new provisions, demands and issues in all different areas of networks.

The solutions that are designed for traditional networks are generally not adequate to deliver proficient adhoc functionality. Further, the wireless type of communication and non-existence of security substructure increase quite a few security issues. The current research in MANETs has grown enormously and is mainly directed towards the need for secure, efficient, scalable and load balancing routing protocols for randomly deployed large-scale environments with high node densities. However, the wise selection of the monitoring nodes chosen for running IDS in conjunction

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 6, Issue 15, April 2026 Impact Factor: 8.2

with trust and machine learning Algorithm based routing techniques for securing dense and sparse adhoc networks has gained attention in respect to designing of power efficient and protected adhoc routing protocols. This thesis aims at designing of secure, decentralized, efficient and scalable security solutions for MANETs, which enable self-configurable and automatic adaption of changes in a network characteristic during its lifetime to detect attacker on early stages. In order to accomplish this objective, the thesis is focused on two areas of MANETs: adhoc secure routing by using Intrusion Detection and cognitive radio mobile adhoc network performance in presence of attacker. The ultimate goal of the thesis is to detect early detection of attack that not only complement the previous routing techniques, but can also be used in MANETs where deployment of the nodes is sparse. Nodes in sparse environment have limited battery power, they keep on moving in the network, and sometimes they do not come in contact with the other network nodes for longer period of time. The application of the proposed algorithms will increase the network performance in terms of efficiency, network lifetime, packet-delivery-ratio and routing-overhead.

Summary

MANETs pose a research challenge in terms of increasing the network lifetime by efficiently using limited resources in a dynamic environment. The important aspect of designing of protocols for MANETs is to make routing protocols secure without impacting the performance and efficiency of the network.

The thesis provides insights in the field of secure, energy efficient, decentralized and scalable communication methods by proposing various new security mechanisms. While using the concepts and studies presented in this thesis, the future research work can be pursued in the following directions:

i. By using the existing work as platform, the proposed work and protocols can be further extended to detect and circumvent other MANET security attacks.

ii. The work can also be modified to make other existing reactive routing protocols secure.

iii. The simulation may be repeated on other proactive protocol such as DSR etc. and its performance may be compared with the reactive protocols.

iv. The work may be extended for the secure routing protocol such as OLSR, DSDV, Adriane, SAR, SAODV etc.

v. In future, the methods proposed in this thesis can be extended with various artificial intelligence and meta heuristic optimization techniques for designing energy efficient and congestion aware routing protocols in wireless networks.

vi. The scope of research work can be extended in the field of mobile sensor networks by considering topology variations due to movement of nodes.

vii. The methods and protocols proposed in the thesis have been validated by the findings of experimental results using NS-2 tool. Further, the simulation parameters used in the work are in line with the specification provided for real testbed experimentation. Thus, the work using the proposed methods can also be extended by using testbed environment.

viii. The validation of fuzzy based intrusion detection may be done using AODV protocol and also extended to other reactive protocols i.e. DSR, SAODV etc.

VI. CONCLUSION

Mobile Ad Hoc Networks provide adaptable communication without relying on fixed infrastructure; however, their dynamic nature and resource constraints expose them to significant security risks. This study examined major security issues in MANETs and assessed existing protection techniques based on efficiency and performance metrics. The results highlight the importance of decentralized, energy-efficient, and reliable security frameworks. The suggested method enhances the capability to detect attacks at an early stage without degrading network performance. These outcomes support the development of secure, scalable, and practical MANET solutions for real-world deployments.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 15, April 2026
Impact Factor: 8.2

BIBLIOGRAPHY

[1] R. Ramanathan and J. Redi, "*A Brief Overview of ad hoc networks: challenges and Directions", IEEE Communication Magazine, vol. 40, issue no. 5,* May 2002.

[2] I. Chlamtac, M. Conti, and J. Liu, "*Mobile ad hoc Networking: Imperatives and Challenges", J. of Ad Hoc Networks, vol 1, issue 1, pp. 13–64,* 2003.

[3] Jeoren Hoebeke, Ingrid Moerman, Bart Dhoedt and Piet Demester, *"An Overview of Mobile ad hoc Networks: Applications & Challenges", Journal of the Communication Networks, pp. 60-66,* July 2004.

[4] Ruchi Makani and B V R Reddy, *"Performance Evaluation of Cognitive Internet on Things under Routing Attacks", International Journal of Sensors, wireless communications and control, vol. 9, pp. 1-10,* 2019.

[5] Daniel G Reina, Sergio L Toral, Federico Barrero, Nik Bessis, Eleana Asimakopoulou, *"The role of Ad hoc Networks in the internet of Things: A case scenario for smart Environments", Internet of Things and inter-cooperative Computational Technologies for collective intelligence, vol 460, series studies in computational intelligence, pp. 89-113*, 2013.