ISSN: 2581-3404 (Online) IF: 5.445 (SJIF)

IJIRTM, Volume-7, Issue-4, August-2023.

# Untethered Connectivity: Navigating the World of MANETs

**Dr. B.K. Verma[1], Dr. Shashi Bhushan[2]**
**Professor, CSE-AI & DS[1], Professor & Director[2]**
**Panipat Institute of Engineering and Technology, Samalkha, Haryana[1]**
**Amity school of Engineering and Technology, Patna, Bihar[2]**
**Email: bkverma.3474@gmail.com[1], shashibhushan6@gmail.com[2]**

**Abstract:** *In this paper, we will discuss the security issues and particular solutions in the mobile ad hoc network. Due to the vulnerabilities of mobile ad hoc network, there are several security problems that exploit its development. We first see the main vulnerabilities in the MANET, which have made it easier to get attacked than the traditionally used wired network. Then we will discuss their security criteria and present the main attack types that exist in it. Finally we will discuss the current security solutions for the mobile ad hoc network.*

**Keywords:** MANET, Intrusion detection system, Security, Secure routing.

## Introduction

In recent years, the growth of mobile computing devices, which may include laptops, personal computers, PDAs and handheld devices, had a revolutionary change in the computing world. Computing will not only trust on the ability provided by these personal computers, and the idea of computing arises and become one of the research mind heads in the computer world . In this computing atmosphere, individual operators utilizes, at the same time and anywhere they may be . The countryside of the universal computing has made it necessary to adopt the wireless network as the interconnection method. The Mobile Ad Hoc Network is one of the wireless networks that have attracted most interest of scientists.

A Mobile Ad hoc NETwork (MANET) is a system of wireless mobile node s that dynamically self-organize in some random and temporary network topologies. People and vehicles can be interconnected in areas without a any existing communication infrastructure. In the MANET, nodes openly communicates with all the others within their communication range while the nodes that are not in the direct range use intermediate nodes to communicate with each other. In these two cases, all the nodes that have participated automatically form a wireless network, therefore this type of wireless network can be viewed as mobile ad hoc network.

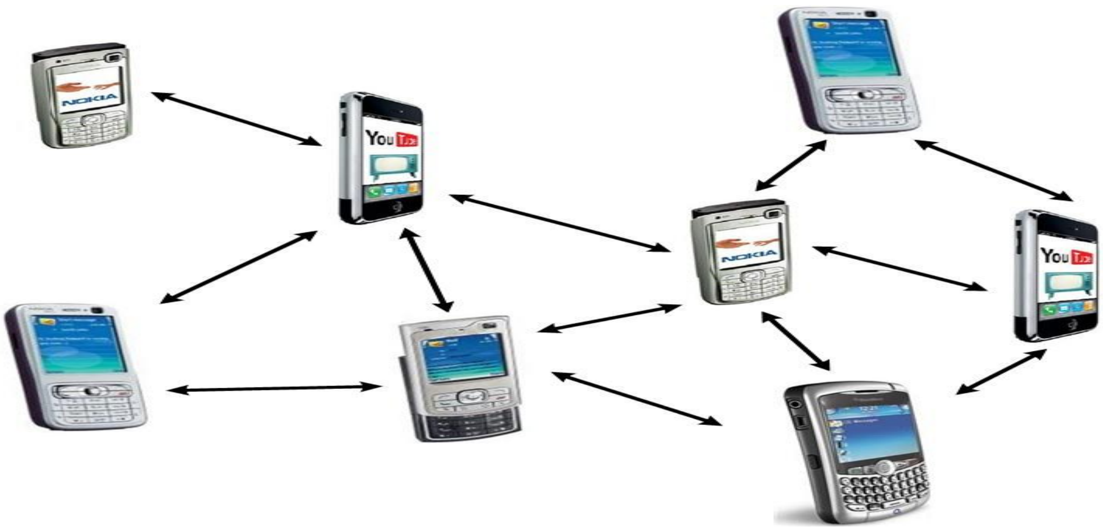

**Fig. 1:** Example of Mobile ad-hoc network.

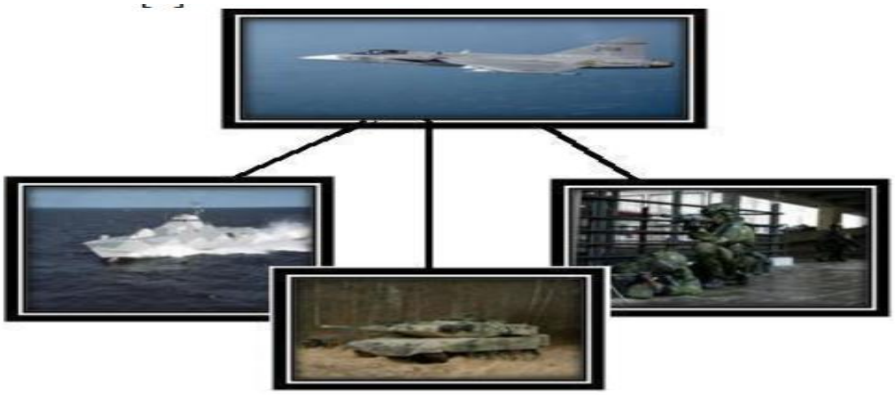

Figure1: Scenario of MANET

**Fig. 2:** Scenario of Mobile ad-hoc network.

## Vulnerability

Since MANET is wireless network and not a wired network so there are many vulnerabilities in the MANET network. Security is much more difficult task in wireless MANET network than from the traditionally used wired network.

## No secure boundary

The meaning of this problem is self-evident: there is not any particular *boundary* in the mobile ad hoc network, which can be related with the defence in the traditionally used wired network. This problem originates from the nature of the manet: liberty to see, join, leave and move inside the network.

### Threats from internal nodes

Since there is freedom for each and every node to join the ad-hoc connection. It is very hard for the nodes to detect the malicious nodes by themselves. Because of the liberty to join it is easy for the node to change the attack target and attack any other node easily. Therefore, threat from the inside node is dangerous than the attacks from the outside the network.

### No Central Management

The absence of the central management makes it much more difficult for the nodes to find the attacks on the system as it is not easy to check the traffic in large scale MANET network.

### Low Power Supply

The nodes in the network will rely only on battery as their power supply technique. While the nodes in the wired network do not need to consider the power supply problem as they always get electric power supply directly from the power buttons. The power supply of wired network is approximately infinite; the nodes in the manet need to consider the restricted battery supply, which will cause many problems.

### Scalability

The scalability problem should be kept in mind as anyone can connect to the network anytime so we do not know how many nodes will be connected in the future. The protocols and services that are to the ad hoc network such as routing protocol and key management service should be well-matched to the constantly changing gauge of the ad hoc network, which may range from two nodes to hundreds of nodes, or even lakhs of nodes.

## Security criteria

Before we check the solutions that will help secure the mobile ad-hoc network, we consider it essential to find out how we should check if a mobile ad hoc network is secure or not. In the following, we briefly introduce the widely-used principles to evaluate if the mobile ad hoc network is really secured or not.

### Availability

The ability to provide all the intended services regardless of the security state of it is termed as *Availability*. This security principle is challenged mainly during the DOS(denial-of-service) attacks, in which all the end points in the wireless network can be attack target and thus some attacker nodes make some of the network services unavailable.

### Integrity

Integrity promises the identity of the messages when they are transmitted. This means that the message should not be lost while sending it through the network and its originality should be maintained throughout the distance.

### Confidentiality

Confidentiality refers to preventing the disclosure of information to unauthorized individuals or systems.Confidentiality means that definite information is only accessible to those who are authorized to access it. In other words, in order to uphold the confidentiality of some private information, we need to keep them secret from all those people that do not have the privilege to access them.

### Authencity

In computing, e-Business, and information security, it is necessary to ensure that the data, transactions, communications or documents (electronic or physical) are genuine. It is essential for the communication members to show their identities as what they have appealed using some techniques so as to guarantee the authenticity. If there existed no authentication mechanism, the opponent could imitate a kind node and thus get access to confidential resources, or even broadcast some fake messages to disturb the normal network operations.

### Nonrepudiation

Nonrepudiation ensures that the sender and the receiver of a message cannot deny that they have ever sent or received such type of message. This is useful particularly when we need to separate if a node with some abnormal behavior is compromised or not. If a node sees that the message it has received is not correct, it can then use the incorrect message as an evidence to notify other nodes that the node sending out the improper message.

### Authorization

Authorization is a method in which an object is issued a credential, which gives the privileges and permissions it has and cannot be forged, by the certificate expert. Authorization is generally used to assign different access rights to different level of users. For instance, we need to ensure that network management function is only accessible by the network administrator. Therefore there should be an authorization process before the network administrator accesses the network management functions.

### Anonymity

Anonymity means that all the information that can be used to identify the owner or the current user of the node should be kept private and not be distributed by the node itself or the system software. This principle is closely related to privacy conserving, in which we should try to protect the privacy of the nodes from arbitrary disclosure to any other entities.

## Security solutions

We have discussed several issues that make the mobile ad hoc networks non secured and attackable in the previous section. However, it is far from our mind and box to secure the mobile ad hoc network if we only know the issues that are existed in it. As then the result, we need to find some proper solutions to the mobile ad hoc network. In this section, we survey some security schemes that can be useful to defend the mobile ad hoc network from nasty behaviours.

**Intrusion Detection**

Intrusion detection is not a new concept in the network research. According to the definition in the *Wikipedia*, an Intrusion Detection System (or IDS) generally detects unwanted operations to systems . Although there are some changes between the traditional wired network and the mobile ad hoc network, intrusion detection technique, which is developed first in the wired network and has become a very important security solution for the wired network, has also gained some eyes from the researchers when they discover the security solution for the mobile ad hoc network. In the following, we discuss  typical intrusion detection techniques in the mobile ad hoc networks in details. Every node in the manet participates in the intrusion detection and activities by detecting signs of malware

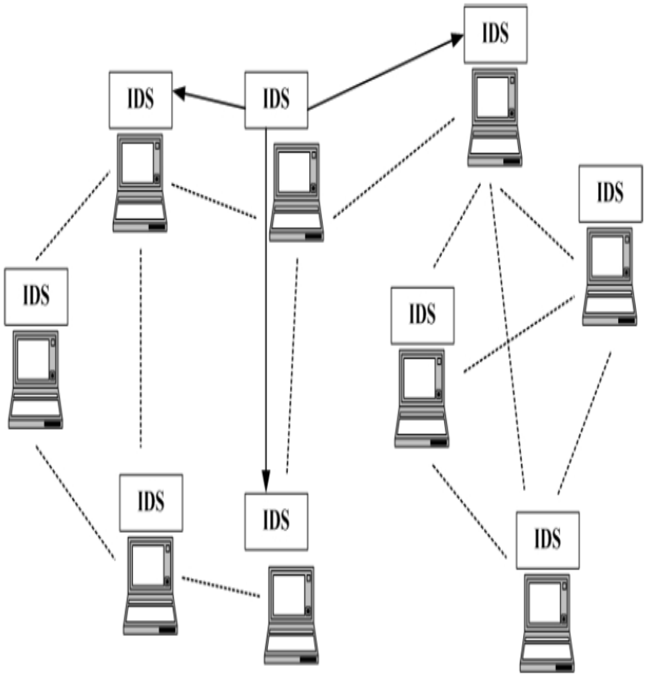

Figure 1. An IDS Architecture for MANET

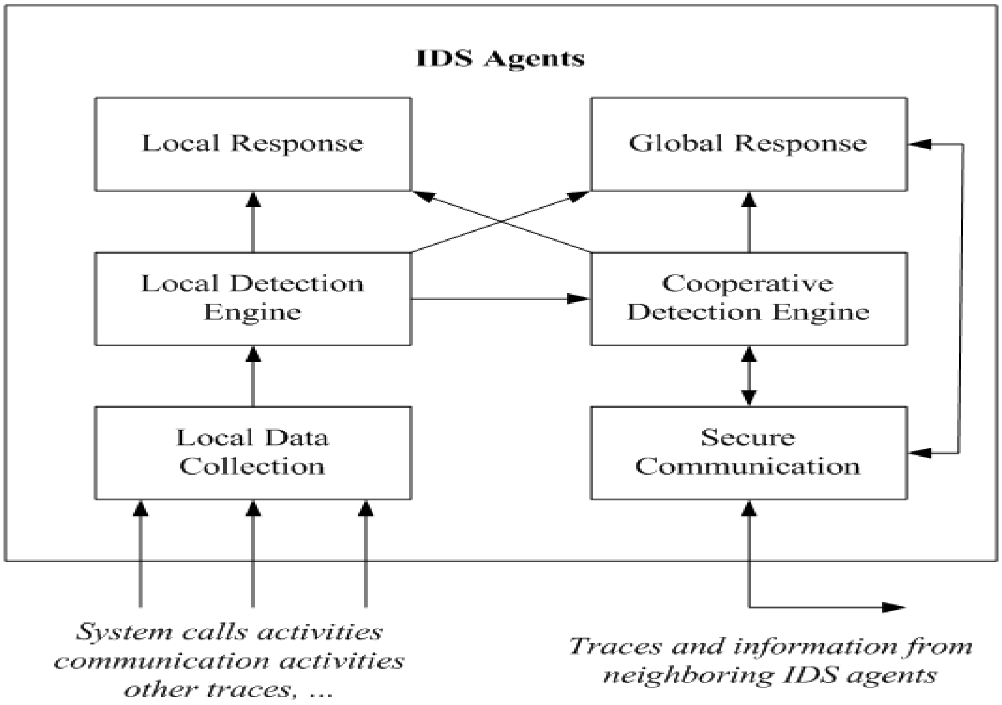
IDS Agents
Local Response
Global Response
Local Detection Engine
Cooperative Detection Engine
Local Data Collection
Secure Communication
System calls activities communication activities other traces, ...
Traces and information from neighboring IDS agents

**Figure 2. A Conceptual Model for an IDS Agent**

behavior locally and globally, which are performed by the built-in IDS agent. However, the adjacent nodes can share their study results with each other and cooperate. The collaboration between nodes usually happens when a certain node detects an irregularity but does not have enough evidence to figure out what kind of stoppage it belongs to. In this situation, the node that has detected the difference requires other nodes in the communication range to do searches to their security records in order to track the possible traces of the burglar.

In our point , there are two points that this technique does not consider, first, is the battery power limitation problem that will cause some nodes to behave in a self-seeking manner during the cooperative intrusion detection process; the second is the obvious overhead that is carried by the multi-layer integrated intrusion detection and response mechanism compared with the original single-layer intrusion detection mechanism.

Misbehaviour Detection through Evaluation analysis

The authors observe the attack actions in the MANET, and find that some *smart* attackers may concurrently feat several weaknesses at multiple layers but keep the attack to each of the vulnerabilities stay below the detection level so as to drip from capture by the single-layer misbehaviour detector. This type of cross-layer attack is far more menacing than the single-layer attack in that it can be easily missed by the single-layer misbehaviour detector. This attack situation can be detected by a cross-layer misbehaviour detector, in which the efforts from all layers of the network stack are joint and examined by the cross-layer detector in a complete way.

There are several aspects that can be further explored in this area. First of all, it will be an significant tricky that how to make the cross-layer detection more well-organized, or in other words, how to collaborate between single-layer detectors to make them work well. Because different single-layer detectors contract with different types of attacks, there can be some unlike viewpoints to the same attack situation when it is experiential in different layers. Therefore it is necessary to figure out the likely solution if there are dissimilar detection results generated by different layers. Second, we need to find out how much the system supply and network overhead will be augmented due to the use of cross-layer detector compared with the unique single-layer detector. Due to the incomplete battery power of the nodes in the ad hoc networks, the system and network overhead carried by the cross-layer detection should be taken into account and likened with the performance progress caused by the use of cross-layer detection method.

## Conclusion

In this survey paper, we try to review the security issues in the mobile ad hoc networks, which may be a main trouble to the operation of it. Due to the mobility and open broadcasting nature, the mobile ad hoc networks are much more disposed to all kind of security risks, such as information disclosure, malware, or even denial of service(DOS). We then debate some typical and dangerous issues in the mobile ad hoc networks, most of which are caused by the characteristics of the mobile ad hoc networks such as mobility, constantly changing topology, open media and battery limitation power. The existence of these issues has made it essential to find some real security solutions and protect the mobile ad hoc network from all kinds of security risks.

## References

[1] M. Weiser, The Computer for the Twenty-First Century, *Scientific American*, September 1991.

[2] M.S. Corson, J.P. Maker, and J.H. Cernicione, Internet-based Mobile Ad Hoc Networking, *IEEE Internet Computing*, pages 63–70, July-August 1999.

[3] Amitabh Mishra and Ketan M. Nadkarni, Security in Wireless Ad Hoc Networks, in Book *The Handbook of Ad Hoc Wireless Networks (Chapter 30)*, CRC Press LLC, 2003.

[4] Lidong Zhou and Zygmunt J. Hass, Securing Ad Hoc Networks, *IEEE Networks Special Issue on Network Security*, November/December 1999.

[5] Yongguang Zhang and Wenke Lee, Security in Mobile Ad-Hoc Networks, in Book *Ad-Hoc Networks Technologies and Protocols (Chapter 9)*, Springer, 2005.

[6] Deepak Kumar Rathore, Dr. Praveen Kumar Mannepalli, "Recent Trends in Machine Learning for Health Care Sector ", International Journal of Innovative Research in Technology and Management, Vol-5, Issue-2, 2021.

[7] R Dubey, D Rathore, D Kushwaha, JP Maurya, "An empirical study of intrusion detection system using feature reduction based on evolutionary algorithms and swarm intelligence methods", International Journal of Applied Engineering Research 12 (19), 2017. pp. 8884-8889.

[8] Deepak Kumar Rathore, Dr. Praveen Kumar Mannepalli, "A Review of Machine Learning Techniques and Applications for Health Care ", International Conference on Advances in Technology, Management & Education, 2021, IEEE proceeding, 978-1-7281-8586-6/21.

[9] Deepak Rathore, Anurag Jain, "Design Hybrid method for intrusion detection using Ensemble cluster classification and SOM network", International Journal of Advanced Computer Research, Vol-2,Issue-3, 2012.