Securing Ad hoc Networks for Intrusion Detection, A study

Shant Kaushik\textsuperscript{[1]}, Sonia Sharma\textsuperscript{[2]}

\textsuperscript{[1]} Assistant Professor, Deptt. of Computer Science, D.A.V. College, Ambala City, Haryana, INDIA
\textsuperscript{[2]} Assistant Professor, Deptt. of Computer Science, Hindu Girls College, Jagadhri, Haryana, INDIA

Abstract:
A Mobile Adhoc Network (MANET) is characterized by mobile nodes, multihop wireless connectivity, Non infrastructural environment and dynamic topology. In Ad Hoc network routing is the reactive on-demand philosophy where routes are established only when required. Stable Routing, Security and Power efficiency are the major concerns in this field. The ad hoc environment is accessible to both legitimate network users and malicious attackers. This paper checks one of the common attack on MANET as Intrusion detection and tries solving the situation.

1.0 INTRODUCTION
Since their emergence in the 1970s, wireless networks have become increasingly popular in the computing industry. This is particularly true within the past decade which has seen wireless networks being adapted to enable mobility. Wireless networks are emerging fast as latest technology to allow users to access information and services via electronic media, without taking geographic position in account. Mobile hosts and wireless networking hardware are becoming widely available and extensive work has been done recently in integrating these elements into traditional networks such as the Internet. Wireless networks have taken the world by storm. Enterprises and homeowners are avoiding the expenses and delays associated with installing wired networks. High-speed Internet facility is enjoyed by travelers all over the places worldwide. Along with increases in throughput, wireless networks remain unlicensed and affordable. This has further helped their exponential growth in businesses, homes, communities and open spaces. There are currently two variations of mobile wireless networks. The first is known as infrastructure networks i.e., those networks with fixed and wired gateways. The bridges for these networks are known as base stations. A mobile unit within these networks connects to, and communicates with, the nearest base station that is within its communication radius. Typical applications of this type of network include office wireless local area networks (WLANs). The second type of mobile wireless network is the infrastructure less mobile network, commonly known as an ad-hoc network.

The term wireless networking refers to technology that enables two or more computers to communicate using standard network protocols, but without network cabling. The technology, with the emergence of cross vendor industry standards such as IEEE 802.11, has shaped a number of popular and cost-effective wireless solutions for business and schools as well as sophisticated applications where installing wired network is impossible, such as in warehousing or point-of-sale handheld equipment. Figure 1 to Figure 3 are representation for various types of wireless networks.

Wireless networks operate in one of the following two modes:
- ad-hoc [IEEE name: Independent Basic Service Set (IBSS)]
- infrastructure [IEEE name: Basic Service Set (BSS)]
In ad-hoc mode, each client communicates directly with the other clients within the network, figure 2:

The main design consideration in Ad-hoc mode is that only the clients within transmission range (within the same cell) of each other can communicate. If a client in an ad-hoc network wishes to communicate outside of the cell, a member of the cell must operate as a gateway and perform routing.

In infrastructure mode, each client sends all of its communications to a central station, or access point (AP). The access point acts as an ethernet bridge and forwards the communications onto the appropriate network—either the wired network, or the wireless network.

2.0 SECURITY NEED

Over a decade or so there have been tremendous changes in the way people communicate. Description of computing device has changed from PC to Communication systems, PDAs, Smart phones. Moreover there are over one billion subscribers using Mobile phone technology as opposed to the number of PCs installed. The new computing devices have the capacity to transmit data in its varying forms, not only to similar devices, but also to different devices across a network. Mobile Internet and mobile network are reality now. The convergence of technologies has made the devices and the network upon which they operate, more interchangeable than ever before with their
overlapping applications. The market is also using latest technology as in E-Commerce which uses B2B (Business to Business), B2C (Business to consumer), G2G (government to government) and G2C (government to citizen) all requiring data exchanges. Also some private communication systems like VPN (virtual private network) and VPA (virtual private access) uses a lot of communication between two networks.

According to IDC sources Global Internet commerce is expected to hit US$ 1 trillion by the end of 2010. With so much abundance of networking, it is becoming more and more needful to have a secured transmission and so security has become a major element in both hardware and the application software. It is being argued that, though a high degree of transmission is already in process, the number would be much greater if data security could be guaranteed. To ensure future growth of markets and their applications, a high degree of security is required, due to potentially high commercial value of both the business and private data. The need for security arises from [6] :

- The growth of mobile internet access and applications
- The individual user requirements
- Corporations (Business or governmental) who both require internal and external contact and data transfer through remote places.

### 3.0 Security Threats

Many organizations—including retail stores, hospitals, airports, and business enterprises—plan to capitalize on the benefits of “going wireless. But if we think about the security of the modern wireless network, this wouldn’t looks so positive. There have been numerous published reports and papers describing attacks on wireless networks that expose organizations to security risks. This section will briefly cover the risks to security—i.e., attacks on confidentiality, integrity, and network availability. Figure 1.10 Provides a general taxonomy of security attacks to help organizations and users understand some of the attacks against ad hoc Wireless network. Network security attacks are typically divided into passive and active attacks [9,10].

![Network Security Attacks Diagram](diagram.png)
The two broad classes of network attacks are then subdivided into other types of attacks, i.e. active attacks and passive attacks. All are defined and briefly discussed as:

**Passive Attack:** An attack in which an unauthorized party gains access to an asset and does not modify its content (i.e., eavesdropping). Passive attacks can be either eavesdropping or traffic analysis (sometimes called traffic flow analysis). These two passive attacks are described below.

- **Eavesdropping:** The attacker monitors transmissions for message content. An example of this attack is a person listening into the transmissions on a network topology between two workstations or tuning into transmissions between a wireless handset and a base station.

- **Traffic analysis:** The attacker, in a more subtle way, gains intelligence by monitoring the transmissions for patterns of communication. A considerable amount of information is contained in the flow of messages between communicating parties.

**Active Attack:** An attack whereby an unauthorized party makes modifications to a message, data stream, or file. It is possible to detect this type of attack but it may not be preventable. Active attacks may take the form of one of four types masquerading, replay, message modification, and denial-of-service (DoS). These attacks are summarized as:

- **Masquerading:** The attacker impersonates an authorized user and thereby gains certain unauthorized privileges.

- **Replay:** The attacker monitors transmissions (passive attack) and retransmits messages as the legitimate user.

- **Message modification:** The attacker alters a legitimate message by deleting, adding to, changing, or reordering it.

- **Denial-of-service:** The attacker prevents or prohibits the normal use or management of communications facilities.

The consequences of these attacks include, but are not limited to, loss of proprietary information, legal and recovery costs, tarnished image, and loss of network service. Due to the dynamically changing topology and infrastructure less, decentralized characteristics, security is hard to achieve in mobile ad hoc networks. Hence, security mechanisms have to be a built-in feature for all sorts of ad hoc network based applications.

In order to make secure the system one should consider the security primary attributes as confidentiality, integrity and availability and secondary attributes as authenticity, non-repudiation and accountability etc. Primary attributes are explained as:

- **Confidentiality** ensures that certain information is never disclosed to unauthorized entities. Network transmission of sensitive information, such as strategic or tactical military information, requires confidentiality. Leakage of such information to enemies could have devastating consequences. Routing information must also remain confidential in certain cases, because the information might be valuable for enemies to identify and to locate their targets in a battlefield.

- **Integrity:** This implies that information cannot be altered except under properly authorized circumstances or it can be said guarantees that a message being transferred is never corrupted.

- **Availability:** This implies that resources are available, where desired or it can be considered that it provides survivability of network services despite denial of service attacks. The entire primary attributes can be maintained in the presence of malicious user and accidental.
Secondary Attribute are explained as:

- **Authenticity**: It implies that apparent identity of the entity is genuine. That is without authentication, an adversary could masquerade a node, thus gaining unauthorized access to resource and sensitive information and interfering with the operation of other nodes.

- **Non-repudiation**: It ensures that the origin of a message cannot deny having sent the message i.e. It implies that authenticity is sufficient trustworthy that later claims to its falsehood cannot be sustained. Non-repudiation is useful for detection and isolation of compromised nodes. When a node A receives an erroneous message from a node B, non-repudiation allows A to accuse B using this message and to convince other nodes that B is compromised.

- **Accountability**: It implies that it is possible to determine what has transpired, in terms of who did what operations or what resources at what time, as desired.

- **Data Freshness**: It ensures that the data is recent and that no adversary replayed old message.

4.0 Existing Solutions

The study is limited in many ways in ad hoc network. Some of the issues that have not been properly addressed, there are many additional issues which have not been addressed for the proper security of ad hoc network. We have proposed the solution for authenticated broadcasting such as data authentication, data confidentiality, data integrity, data freshness, non-repudiation; these are security goal for any application to be achieved. Some of the measures that can be incorporated are:

1. **Virtual Private Networks (VPN)**: This offers a solid solution to many security issues, where an authenticated key provides confidentiality and integrity for IP (Internet Protocol) data grams. Software are available to implement VPNs on just about every platform. Authentication depends upon three factors as password, Fingerprints and a security Token. Using two factors is desirable and using all three is most secured. VPN only support IP suite so it cannot be solution for all environments.

2. **Encryption**: Encryption is a technique used for many years for passing information from one place to other in a secured manner. A message in its original shape is referred to as a plaintext (or Text) and a message used to conceal original message is called Ciphertext (or Cipher). The process of changing plaintext into ciphertext is called Encryption and the reverse process is called decryption. There are many algorithms available for these processes. Some of them are Data Encryption Standard (DES), International Data Encryption algorithm (IDEA) and Public key algorithm (RSA) These are based on key based algorithms. There is one popular key algorithm as Digital signature algorithm. In Digital signature, Signer encrypts the message with key, this is sent to recipient, the message is then decrypted with sender’s public key. In case of ad hoc networks this may not be the best method as it uses a lot of space and is also slow.

3. **One Way Hash Function**: There is another algorithm called One way hash Function: it is like checksum of a block of text and is secure in that it is impossible to generate the same hash function value without knowing the correct algorithm and key. It accepts a variable size message and produces a affixed size tag as output. This algorithm can be combined with encryption to provide an efficient and effective digital signature.

4. **Digital Signature**: External attacks can be checked using Confidentiality of the routing information and also by authentication and integrity assurance features. Encryption can be solution to this. Digital signatures and one way functions can be applied. Permian used complex robustness to
protect routing data from compromised nodes. It is ability to continue correct operation in presence of arbitrary nodes with complex failures.

5.0 Intrusion Detection System (IDS)
Intrusion detection can be describe informally as a security mechanism which attempts to identify those who are trying to break into and misuse a system without authorization and those who have legitimate access to the system but are abusing the privilege.

Prevention based approaches can significantly reduce potential attacks; however they cannot totally eliminate intrusion. The aftermath of a node attack left the node more open to attacks. This renders the prevention-based technique less resilient to malicious attacks. Practically insiders can cause greater damage. Therefore, intrusion detection systems (IDSs) are required for providing a highly-secured system as the second line of defense.

5.1 Types of Intrusion detection system
Generally there are two common types of intrusion detection: anomaly-based detection and misused –based detection. Also we discuss the third, which is a hybrid form of IDS.

(a) Anomaly based detection. An anomaly-based detection technique creates normal profiles of systems states or user behaviors and compares them with current activities. The normal profiles (or normal behaviors) of users are kept in the system. The system compares the captured data with these profiles and then treats any activity that deviate from the baseline as possible intrusion by informing system administrators or initializing proper responses. The main advantage of anomaly-based detection is that it does not require prior knowledge of intrusion and can thus detect new intrusions. The main disadvantage is that it may not be able to describe what the attack is and may have high false positive rate.

(b) Misuse-based detection. A misuse-based detection encodes known attack signatures and system vulnerabilities and stores them in a database. If deployed IDS find a match between current activities and signatures, an alarm is generated.

(c) Specification-based detection: A hybrid based- detection known as specification-based detection combines the advantages of misuse detection and anomaly detection by using manually developed specifications to characterize legitimate system behaviors. Specification-based detection approaches are similar to anomaly detection techniques in that both of them detect attacks as deviations from normal profile.

5.2 Functions of Network Intrusion Detection
Intrusion detection systems are designed to enhance fact finding operations in computer systems, the goal is to help accomplish the task of searching and detecting of attacks by collecting related information from a variety of system and network sources, thereafter analyzing the collected information for symptoms or traces of security disorders. The IDS provides the following functions:

- Auditing of system configurations and vulnerabilities
- Monitoring and analysis of user and system activities
- Assessing the integrity of critical system and data files
- Recognition of activity patterns reflecting known attacks
- Statistical analysis for abnormal activity pattern.
- Operating system audit trial management with recognition of user reflecting policy violations
6.0 Proposed plan

If cryptography is used it takes many bits thus reducing the speed. Different protocols available pose different threats to their security and use different measures to solve them. Not one method is available which can solve most of the problems if not all. Our purpose for this study is to combine major features of two or three schemes so that it can work for most of the available protocols in terms of protection. The proposed scheme will incorporate the basic idea to develop a new scheme to fit in most of the environments. In addition to this, there are some aspects which we are trying to cover as Overhead caused by adding security parameters. Speed of data transmission, which will be affected due to added size. Also medium of transmission is to be taken care of, which can be denser or sparse. An effort has been done to incorporate the security parameter as “key encryption” to existing routing protocols and see the effect of it. The major issue is overhead and speed of data transmission. The work will enable a flexible topology control framework that utilizes nodes and data aggregation network topologies with reduced energy consumption required to improved network security level.

The basic idea is to implement an intrusion detection system required to detect the presence of a jammer attack within the network. The proposed scheme will follow a three-phase structure for the implementation process.

- First an algorithm will be employed with the formation of a route creation path.
- Second the neighbour discovery phase will be performed and Finally the detection algorithm based on related attacks and classifications of normal and abnormal profiles will take into consideration a jammer attack process.

Acknowledgment: Authors are thankful to Dr Ashwani Kush, head, dept of computer science, UC KUK India for their valuable support and advice.

REFERENCES

2. Hamalainen, Panu Henrikki, Tampereen Teknillinen Korkeakoulu (Finland) “Wireless Local Area Networks”, 1994
7. Wang, Weichao from Purdue University, works on the Securing Wireless Network Topology and Routing, 2005
12. Showrank, Jamie Marie from Robert Morris University, Network Security Framework For Web Content Maintenance, 2005


