A Survey on Security and Through-Put Relay in Mobile Mesh Networks

1.Srinivasan.J
Research scholar,
St.Peters University,
Chennai.

2.Dr.Audithan.S
professor,
Prist University,
Kumbakonam.

Abstract— Networks composed of mobile nodes inherently suffer from intermittent connections and high delays. Performance can be improved by adding supporting infrastructure, including base stations, meshes, and relays, but the cost-performance trade-offs of different designs is poorly understood. To examine these trade-offs, we have deployed a large-scale vehicular network. Mobile ad-hoc networks (MANETs) are ideal for situations where a fixed infrastructure is unavailable or infeasible. Today's MANETs, however, may suffer from network partitioning. This limitation makes MANETs unsuitable for applications such as crisis management and battlefield communications..A Mobile Ad hoc network (MANET) is a dynamically arrangement of wireless Mobile nodes, communicate directly or using intermediate nodes without any predefined infrastructures. In the absence of any predefined infrastructures in networks become vulnerable to number of attacks and high level security becomes a major issue. In this survey paper, we first discuss about the introduction to Mobile Ad hoc network. The second section discusses the weaknesses or vulnerabilities in Mobile Ad hoc network. The third section discusses the types of attack in Mobile Ad hoc network. The fourth section discusses about a new class of ad-hoc network called Autonomous Mobile Mesh Network (AMMNET) for Through-put Relay. Finally the last section discusses about the simulation results of AMMNET proves robust against network partitioning and capable of providing high relay throughput for the mobile clients.

Keywords— AMMNET, Mobile Ad Hoc Networks, Attacks, Security, Solutions.

1. INTRODUCTION

Ad hoc wireless networks are interconnected sets of mobile nodes that are self-organizing, self healing, survivable, and instantaneously available, without any need for prior infrastructure. Since Internet Protocol (IP) suite is now recognized as the universal interface or "glue" for interconnecting dissimilar Networks, an IP-based ad hoc network has the potential to solve the interoperability problems faced by various conventional stovepipe networks that are designed for specific usage cases. A multi-hop mesh network can be defined as a communications network that has two or more paths to any node, providing multiple ways to route data and control information between nodes by "hopping" from node to node until a connection can be established. Mobile mesh networks enable continuous efficient updates of connections to reconfigure around blocked or changed paths. WIRELESS technology has been one of the most transforming and empowering technologies in recent years. In particular, *mobile ad-hoc networks* (MANETs) are among the most popularly studied network communication technologies. The mobile nodes also play the role of the routers, helping to forward data packets to their destinations via multiple hop relay. This type of network is suitable for situations where a fixed infrastructure is unavailable or infeasible. One great challenge in designing robust MANETs is to minimize network partitions. As autonomous mobile users move about in a MANET, the network topology may change rapidly and unpredictably over time and portions of the network may intermittently become partitioned. We address this challenging problem in this paper by proposing a new class of robust mobile ad-hoc network called *Autonomous Mobile Mesh Networks* (AMMNET) under Section-IV. Mobile Ad hoc networks have different types of features as follows [4]: Firstly, the main features of an Ad hoc network are that there are temporary and do not require any cabling. Secondly, there is unfaithfulness of wireless link between the nodes. The Ad hoc networks are not faithful for the communication nodes because of limited intensity supply for the wireless nodes. Thirdly, the rapid changes in the routing topology due to continuous move and change in the position of nodes. This means that the nodes have the ability to move in or outside the transmission range of the nodes in Mobile Ad hoc network. [Figure 1] Shows Mobile Ad hoc network.

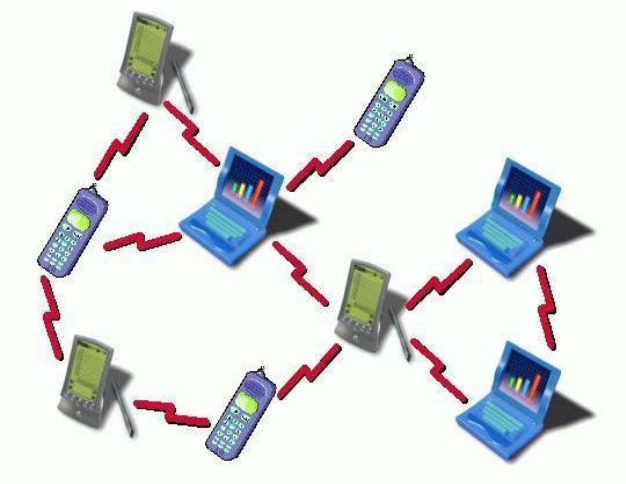

Figure 1: MANET Architecture.

Therefore, because of the features listed above, we need to pay attention to the security issue in the Mobile Ad hoc Network. The rest of the paper is organized as follows: The second section discusses weaknesses or vulnerabilities in Mobile Ad hoc network. The third section discusses the types of attack in Mobile Ad hoc network. The fourth section discusses the Waiting time and through put relay of Mobile Ad hoc network. Finally the last section discusses the Stimulation Results and Conclusion.

2. VULNERABILITIES OF THE MOBILE AD HOC - NETWORKS

2.1 Insecure Architecture

The Mobile Ad hoc network is insecure by its nature. There is no such restriction for nodes to joining, leaving and moving inside or outside of the network, thus the lack of security makes the Mobile Ad hoc network vulnerable to the attacks. The Mobile Ad hoc network becomes wide open as there is no line of defense such as firewall and gateway before they can perform malicious behavior to the targets [6].

2.2 Variable Topology

Mobile Ad hoc network nodes are independent: They can leave or join any network. As a result the topology changes regularly. It is hard to track the malicious behavior performed by a node in a network. Therefore, threats from these nodes inside the network are more dangerous than that the attacks from the outside attackers and these attacks are hard to detect.

2.3. Possibility of Centralized Management

Mobile Ad hoc network do not have any centralized management facility such as a name server, which leads to some vulnerable problems. The unavailability of centralized management machines makes it indeed very hard to detect attacks because it is hard to monitor the traffic in a highly dynamic and large scale Mobile Ad hoc network [7]. This problem affects in turn breakdown and failure in transmitted data. There is no involvement of the nodes in any security operations. A shortage of this type cause directly all operations of Mobile Ad hoc network especially when there is any serious attack faced by any node [5][14][7].

2.4. Limited Power Supply

The nodes in Mobile Ad Hoc Network rely fully on the battery as their power supply method, which is bounded kind of power supply. And so, any types of failure in Mobile Ad hoc network instantly cause many problems. But in contrast, the wired network does not need any power supply because it gets its power directly from the electronic power supplier. The first problem occurs is denial-of-service attacks [4]. The second problem is caused by some node suffering from the running off battery power, this behavior is literary a selfish behavior in Mobile Ad hoc network [8].

2.5 Increasing Scalability

In general wired network scale is predefined when designed and not change such during the use, but Mobile Ad hoc network scale is changing all the time because of mobility of the nodes in Mobile Ad hoc network.

3. ATTACK TYPES IN MOBILE AD-HOC NETWORKS

There are numerous types of attacks in the Mobile Ad hoc network, which can be classified as the following two main types [6]:

A. External attacks, in which the attacker aims to propagate fake routing information, cause congestion or disturb nodes from providing services.

B. Internal attacks, in which the attacker wants to participate in the network activities and gain the normal access to the network, by some malicious acting to get the access to the network as a new node, or by directly communicating a current node and using it as a basis to conduct its malicious behaviors. External attacks are similar to the regular attacks in the long established wired networks in that the attacker is in the closeness but not a trusted node in the network, therefore, this type of attack can be stopped and detected by the security methods such as authentication or firewall, which are relatively traditional security solutions.

3.1 Eavesdropping Attacks

Eavesdropping is known as disclosure attacks, usually done by external or internal nodes and is passive. The attacker's goal of eavesdropping is to analyze broadcast messages and obtain some useful information about the network that is secret during the communication [9].

3.2. Denial of Service (DoS)

The second type of attack is denial of service; in this attackers try to attack at the availability of services of the entire Mobile Ad hoc network. The attackers use the battery exhaustion methods and the radio jamming to perform DoS attacks to the Mobile Ad hoc network.

3.3. Dropping Attacks

In Mobile Ad hoc network nodes those are malicious or selfish nodes deliberately drops all the packets that are not destined for them. In dropping attack, malicious nodes aim to disrupt the connection, whereas selfish nodes aim to preserve their resources. It reduces the network performance by causing data packets to be transmitted again, new routes to the destination is to be discovered.

3.4. Attacks against Routing

Routing is one of the most important part in Mobile Ad hoc network, it the one of the main targets of attackers. Attacks on routing protocols are classified as attacks on protocols and on packet forwarding or delivery [07]. It is very difficult to validate message in constantly changing topology of the Mobile Ad hoc networks. There are some more sophisticated attacks on routing includes Wormhole attack & rushing attacks.

4. WEAKNESS AND THROUGH PUT RELAY IN MOBILE AD HOC NETWORKS

AMMNET is a standard wireless mesh network; stationary mesh nodes provide routing and relay capabilities. They form a mesh-like wireless network that allows mobile mesh clients to communicate with each other through multi hop communications. Such a network is scalable, flexible, and low in maintenance cost. When a mesh node fails, it can simply be replaced by a new one; and the mesh network will recognize the new mesh node and automatically reconfigure itself. The mobility of the mesh clients is confined to the fixed area serviced by a standard wireless mesh network due to the stationary mesh nodes. In particular, an *AMMNET* tries to prevent network partitioning to ensure connectivity for all its users. This property makes *AMMNET* a highly robust MANET.

The issues discussed so far ensures that the mesh nodes maintain the connectivity for all clients. The resulting networks, however, might incur long end-to end delay with potentially many unnecessary intergroup routers because the bridging networks are constructed independently. As an example shown , if a client in group G2 wants to communicate with another client in group G3, this must be done through a long path over the router b1 at group G1 although groups G2 and G3 are near each other. Another potential drawback is the excessive use of the intergroup routers. To improve this condition, there are 2 proposals two topology adaptation schemes, namely local adaptation and global adaptation, each with a different resolution of location information to shorten the relay paths between groups.

5. STIMULATION RESULTS

Intuitively, there are two strategies for stationary node placement based on regions in the mobile network.
Uniform placement: place the nodes uniformly across the entire network limited only by the placement constraints described above.
• Non-uniform: place more nodes in the network core, while still following the placement constraints. We use a simple heuristic for such a placement. The number of nodes in each square (see Figure 3) is proportional to the amount of time mobile nodes spend in that square.

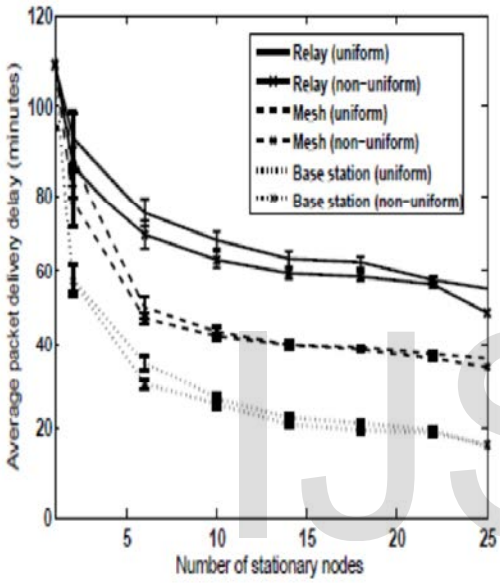

Figure 2: The average packet delivery delay with a varying number of stationary nodes for uniform and non uniform
Placement.

6. CONCLUSION

In this survey paper, we try to survey the security issues in the mobile ad hoc networks, which may be a main issue to the operation of Mobile Ad hoc Network. Due to the insecure nature and dynamic topology, the mobile ad hoc networks are less secure to all types of security risks, such as information disclosure or denial of service. As a result,
the security needs in the mobile ad hoc networks are much higher than those in the regular wired networks. Then We have performed an experimental and analytical study of mobile networks enhanced with relays, meshes, and wired base stations. We first explore the trade-offs with each type of infrastructure experimentally in the context of a deployed vehicular test bed. However, since the number of mobile and stationary nodes in the deployment is small, we Complement this effort by developing analytical models of large-scale networks in the presence of different infrastructures. Based on the model and the deployment, our study draws three main conclusions. (1) We need less than 5–7 times as many relays and 2–3 times as many mesh nodes as base stations for a similar enhancement in performance.

REFERENCES

[1]. Marco Conti, Body, Personal and Local Ad Hoc Wireless Networks, in Book The Handbook of Ad Hoc Wireless Networks (Chapter 1), CRC Press LLC, **2003.**
[2]. M. Weiser, The Computer for the Twenty-First Century, Scientific American, September**1991.**
[3]. 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.**
[4]. Amitabh Mishra and Ketan M. Nadkarni, Security in Wireless Ad Hoc Networks, in Book The Handbook of Ad Hoc Wireless Networks (Chapter30), CRC Press LLC, **2003.**
[5]. Lidong Zhou and Zygmunt J. Hass, Securing Ad Hoc Networks, IEEE Networks Special Issue on Network Security, November/December **1999.**

[6]. Yongguang Zhang and Wenke Lee, Security in Mobile Ad-Hoc Networks, in Book Ad Hoc Networks Technologies and Protocols (Chapter 9), Springer, **2005.**
[7]. Panagiotis Papadimitraos and Zygmunt J. Hass, Securing Mobile Ad Hoc Networks, in Book The Handbook of Ad Hoc Wireless Networks (Chapter31), CRC Press LLC, **2003.**
[8]. Yi-an Huang and Wenke Lee, A Cooperative Intrusion Detection System for Ad Hoc Networks, in Proceedings of the 1st ACM Workshop on Security of Ad hoc and Sensor Networks, Fairfax, Virginia, **2003**, pp. 135 – 147.
[9]. Data Integrity, from Wikipedia, the free encyclopedia,http://en.wikipedia.org/wiki/Data_integrity.
[10]. P. Papadimitratos and Z. J. Hass, Secure Routing for Mobile Ad Hoc Networks, in Proceedings of
SCS Communication Networks and Distributed Systems, **2002**.