CHAPTER 1

INTRODUCTION

In recent decades, the use of wireless communication has tremendous growth in real life applications because of its distinctive features such as easy to installation, mobility etc. Also wireless communication has various limitations like limited energy, bandwidth, signal capacity etc. The wireless communication is confronting of various security issues and any standard full proved security model is still not defined.

1. Introduction

Presently, there is a high growth in the use of wireless communication. The major advantage of wireless communication is the ability to transmit data among users with mobility. However the distance between nodes are limited by the signal strength of the transmitter. If signal strength is more the area covered by the network will be more and vice-versa. This problem can be resolved by Mobile Ad-hoc Networks (MANET) by allowing out of range nodes to access network by using intermediate hop nodes. Ad-hoc Network is a temporary network created and operated by the nodes themselves without having any centralized infrastructure. Nodes cooperate with each other by passing data and packets from one hop to another. Every nodes act as a router itself for communication purpose. MANET is a multi-hop wireless network with limited battery power, limited bandwidth and dynamic topology. MANET networks have many applications in military, commercial and in personal area network. The use of ad-hoc network is justifiable in situation where installing infrastructure is not always possible such as in war zone or disaster management like storm, earthquake. Also ad-hoc nodes can be connected to a fixed backbone network by using gateway devices providing IP network services. Ad-hoc network improves the throughput performance by using all the nodes for routing and forwarding data and control. So selecting appropriate routing technique is a difficult task as the conventional routing algorithm cannot be directly used for ad-hoc network because of the dynamic feature. Due to dynamic nature of nodes, topology changes frequently at any time. So it is very difficult to find an optimal route for communication. The routing algorithm must act quickly as the topology changes. Different protocols have been developed for such type of network. But due to dynamic nature of the network, the topology changes frequently and the network is open to attack and unreliability. Nodes misbehavior due to malicious intention could radically reduce the performance of MANET. Due to openness and dynamicity of ad-hoc network security is a key problem. Ad-hoc networks having various issues like access control, authentication, reputation, trust, integrity, availability etc., which requires security issues. In real life situation all nodes may not be cooperative, which leads to malicious act. Since the nodes act as a communicating device in a wireless environment, so trust is a major factor in MANET. Ad-hoc network communicate depending upon the cooperative and trusting nature of nodes, so trust is a major concern in this network. Trusted routing will identify the malicious node and will exclude them from participating in the routing mechanism of the network. The main focus of this research work is to develop trust model that is trusted routing protocol which can secure the network against malicious behaviors of nodes.

1.1 Ad-hoc Network

An ad-hoc network is a temporary network formed by mobile or semi mobile devices without having a pre-established network. Each of the device participated in the network communicate with each other via intermediate nodes. For communicating among mobile nodes radio or infrared are used. Laptops and Personal Digital Assistants (PDA) etc. are some of the devices that may be used in an ad-hoc network. Nodes in ad-hoc networks are generally of mobile nodes but can also consist fixed nodes for access point to the internet. The nodes can act both as host as well as router in an ad-hoc network.

Ad-hoc network has the feature of handling dynamic topology. For example if any node leave a network which causes link breakage, the disconnected node will send new route request and the network will be reconfigured and will be operational again. Ad-hoc network having also the advantage of wireless communication without having restrictions of wired communication, if any two nodes are within the transmission range, a link will be automatically created within them. The Figure 1.1 shows an example of ad-hoc network where five nodes formed a network in wireless environment.

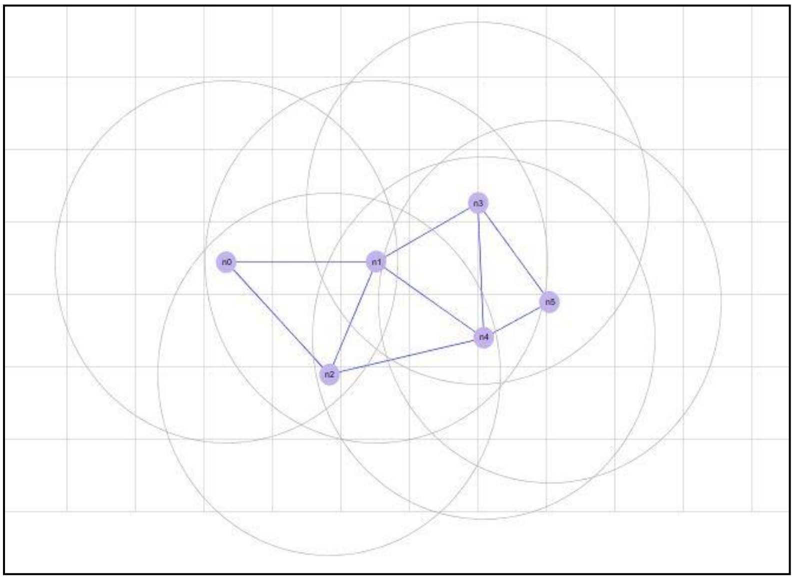

Figure 1.1: A simple example of Wireless Ad-hoc Network

1.2 Mobile Ad-hoc Network (MANET)

MANET (Murthy and Manoj, 2008) is a set of mobile devices (nodes), establish a network themselves and communicate with each other with wireless medium without the presence of a predefined infrastructure or a central authority. Because of the mobility associated with ad-hoc networks, they are commonly called MANET (Mobile Ad-hoc Network). MANET can be set up anywhere any time because it does not require any preexisting infrastructure. Since, nodes are self-organized and self-configured any node can join or leave the network.

MANETs are applicable in the situation where establishing fixed network is impossible or costly. MANET can also be used where infrastructure is damaged or destroyed such as warzone, battlefield, flood affected area, disaster relief team. MANET can also be used as civilian environment such as classrooms, conferences, research areas.

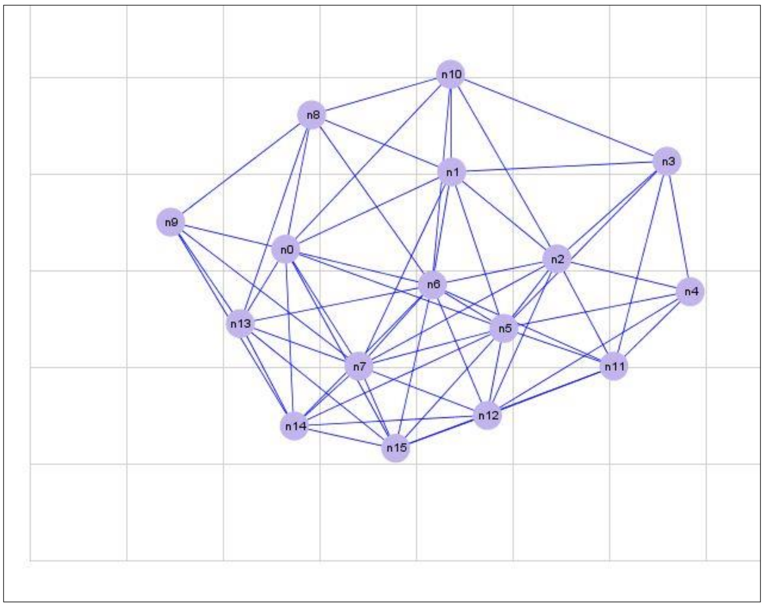

Figure 1.2: A graph representing a MANET of 15 nodes

Figure 1.2 is an example scenario of MANET showing the network connectivity of fifteen mobile nodes with wireless link. Every node discovers their communicating path via intermediate hop.

1.2.1 Characteristics and Challenges of MANET

The main characteristics of MANETs (Venkataraman and Pushpalatha, 2006; Royer and Toh, 2002) can be classified as follows:

a) **Cooperativeness:** Nodes in MANET are cooperative in nature. So the malicious nodes can easily join the network and can disrupt the network resources by not obeying the network protocols specification.

b) **Dynamism of Topology:** The nodes of MANET are randomly, frequently and unpredictably mobile. Any node can join or leave the network at any time. Since the nodes leaves the network at any point of time, so link breakage may occur, but the nodes of the MANET reconfigured and disconnected nodes can be connected to the network via new route.

c) **Lack of Fixed Infrastructure:** MANET doesn’t have any centralized infrastructure. Due to the lack of existing infrastructure, the existing techniques of network are not feasible for MANET.

d) **Resource Constraints:** The mobile devices used in MANET have various resource constraints like limited battery life, limited transmission range, communication range, computational power, memory bandwidth etc. So in order to achieve a reliable communication between nodes, these resource constraints affect much for better performing of the network.

e) **Lack of Centralized Management:** MANET does not have any centralized management node. So, detection of malicious behaviors become complex in a dynamic and large network.

f) **Scalability:** Since the nodes are mobile so the scale of the networks varies from time to time. Security technique should be able to handle small as well as large scale networks.

g) **Limited Power Supply:** The nodes in MANET have limited power supply, which may cause various problems like as selfish behavior.

h) **Bandwidth Constraint:** Since there may exist low capacity links among the nodes, so interference, external noise, signal attenuation affects are vulnerable to network.

i) **Adversary inside the Network:** Since MANET is an open network, anyone can join and leave the network freely, and the participating nodes in the network may act maliciously, which is more dangerous than external attack.

j) **No Predefined Boundary:** In MANET there is a fixed boundary. Anyone can join the network when it comes into the coverage area of the network.

1.2.2 Applications of MANET

MANET has wide range of application areas due to the increase of mobile devices like laptop, PDA etc. MANET can be used anywhere where there is no infrastructure or using infrastructure is not possible or cost effective. MANET allows the devices to easily connected or disconnected from the network. MANET application set includes large scale networks, small scale networks, and fixed power constraint networks, mobile and highly dynamic networks. Major application areas of MANET include:

a) **Military Battlefield:** MANET can be used in military battlefield. MANET can be used to make communication network between the soldiers, vehicles, and information headquarters. Ad-hoc networks can also be used in soldiers, tanks, planes etc.
b) **Commercial Sector:** MANET can be used in emergency situation for rescue operation in disaster management like fire, flood, storm, tsunami, and earthquake. In emergency situation where there is no communication or communication has been damaged ad-hoc network can be easily deployed. Other commercial application includes ship to ship mobile communication, law enforcement, vehicular ad-hoc network etc.
c) **Local Level:** Ad-hoc networks can be used to share and communicate among group of participants like classroom or conference room. Other local level application areas include home network, taxi cab, stadium, boat, small aircrafts etc.
d) **Personal Area Network (PAN):** MANET can be used for interconnecting various mobile devices like palmtops, laptops, cellular phones etc. Ad-hoc network can also access the internet from other network mechanism such as Wireless LAN (WLAN), GPRS, and UMTS etc.
e) **MANET Voice over Virtual Overlay Network:** This is a new application of MANET. In JXTA (Luis Bernardo et. al.,) open platform, MANET is used to find user location and also used for audio streaming over the JXTA virtual network. Using MANET-JXTA, a client can search for a user and call setup until a destination user is reached.

1.2.3 Current Status of MANET

Ad-hoc network concept is not a new; rather it has started in 1970's by military force. In recent decades commercial interest has grown tremendously due to the advancement of mobile devices and wireless technologies. In Internet Engineering Task Force for developing mobile nodes routing and for a framework for running IP based protocols in MANET (Chlamtac *et. al.,* 2003) a group has been created. Many national and international conferences, symposium and workshop held in MANET by IEEE and ACM like Mobi Hoc (The ACM Symposium on Mobile Ad-hoc Networking & Computing), ACM SIGMOBILE , which is a special interest group on mobility of systems, users, data and computing). IEEE 802.11 standard has increased research interest on this field. Researchers from various industry, academic institution and government are having much attention on this field because of its wide scale application. Since MANET has many research issues and challenges so research in this field is still an open problem.

1.2.4 Comparison of Infrastructure and Ad-hoc Networks

In an infrastructure network, stations are required to be in the coverage area of access point. Therefore, nodes mobility is limited within the range of the access point. But, in an Ad-hoc network, a station can transmit data to outside of the range of a device by communicating through intermediate nodes.

In an infrastructure network battery usage optimization can done by keeping the stations in power saving mode. But in ad-hoc network batter power is low but consumption is high.In an ad-hoc network topology changing is permissible so any time any node can join or leave the network, but in infrastructure network it is not always possible.

1.3 Motivation

In the present era of communication network, MANET is popular because of its wide range applications in many infrastructures-less environments and applications; mainly in complex settings, such as: vehicular, emergency rescue, as well as military and law enforcement. MANETs are popular because of availability of low cost mobile devices and easy to set up wireless network where installation of wired network is not always possible or takes cost. MANETs are susceptible to various attacks because of changing topology, limited resource and unavailability of any centralized infrastructure. MANET always confronts security and selfishness issues because of self-organizing problem and resource constraints. The motivation here focuses on to design trusted routing protocols using trusted frame works (secure protocol) for MANET. In real life in some places, we find that there is no network coverage, also if it exists, in some special situations it does not work properly. For example, in emergency situations like rain storm, hurricane, tornado, tsunami the existing network will damage, so in that situation instantly we can setup a network using MANET. Also this network can be used in military services. In geographically backward regions like Barak Valley, there are many places where still there is no network coverage, so government and people faces many problems in communications in various situations like at the time of emergency or at the time of election processes, or to communicate to a group of peoples in an industrial area. We can use this network in such type of circumstances. But although MANET has been developed no full proof security model is developed, till various security problems exists. Such type of real life applications motivate me to work in this area.

1.4 Objectives

The main objective of my research is to develop comprehensive models for security attacks and a trustworthy security framework against security attacks in an ad-hoc network. This evaluation has been done theoretically and through simulation. This simulation environment should be based on Network simulator 2 (http://www.isi.edu/nsnam/ns/).

The objectives of this research are:

a) To analyze the protocols theoretically and through simulation.
b) To construct secure and efficient privacy-preserving routing protocols in MANETs.
c) To develop trust based security models which will reduce the effect of routing attacks in MANET.

1.5 Major Contributions

a) Studied various MANET routing protocols and its behaviors.

b) Studied various MANET routing attacks.

c) Compare the performance between proactive and reactive routing protocols through simulation.

d) Developed a trusted routing protocol named Secured Routing Using Trust Estimation Model (SRUTEM) using trust estimation function.

e) Redesign SRUTEM with modified feature as TSRM.

f) Developed a trust based routing protocol for mitigating blackhole attack using trust function.

g) Developed a trust based routing protocol for resisting grayhole attack.

h) Developed a recommendation based trust model for resisting dishonest recommendation problem.

i) Analyze the results, and drawn conclusions of the work.

1.6 Thesis Outline

The rest of the thesis is organized as follows:

Chapter 2: Literature Review: This chapter deals with detailed survey about various trust model, various routing attack prevention mechanism like blackhole, grayhole, wormhole, flooding attack prevention techniques etc. This chapter also presents a simulated comparison between proactive and reactive routing protocols. Here we have compared DSR and DSDV in terms of Packed Delivery Fraction, Normalized routing load and average end to end delay. A part of this chapter is published in Assam University Journal of Science and Technology, ISSN- 0975-2773, 8(II), 70-74. (Kefayat *et al.*, 2012).

Chapter 3: Secure Routing in MANET using Trust Estimation Model: In this chapter we have developed one routing algorithm using trust estimation function. In the process we have defined a trust function based on experiences. This trust function is integrated into the Dynamic Source Routing (DSR) protocol. The performance of the proposed protocol is evaluated by comparative analysis of result with the standard

DSR protocol in presence of malicious nodes. A part of this chapter is published in conference proceeding NCRTCSA, bonfring. (Kefayat *et al.*, 2014).

Then again the proposed model is modified. Here we have combined both Blind Trust and Referential Trust using a function. Also we have tested the performance of our new developed protocol with the existing one with different parameters. The improved technique is published in conference proceeding, IEE. (Kefayat *et al.* 2015).

Chapter 4: Mitigating Blackhole Attack in MANET using Trust: This chapter deals with trust based mechanism to mitigate blackhole attack. Here, the DSR header file is modified to measure trust in the network. The proposed TIDSR improves the network performance without compromising to security although it has increased the intermediate hop count little more. The proposed model can be extended for other protocol as well as for mitigating other malicious attack.

Chapter 5: Trust Based Routing for Mitigating Grayhole Attack in MANET: In this chapter we present a Trust Based DSR (TBDSR) to mitigate packet dropping that is grayhole attack. In the process first the nodes trust value is calculated using the trust calculating function, then the DSR RREQ header and RREP header were updated. Based on trust value and threshold value the optimal route has been selected for routing. Finally the performance were measured based on various performance parameters. A part of this chapter is published in International Journal of Information Science and Computing, ISSN NO: 2348-7437, 3(1), 1-9. (Kefayat and Das, 2016)

Chapter 6: An Improved Trust Model for Mitigating Dishonest Recommendation Problem: This chapter presents a probabilistic trust model which mitigates dishonest recommender nodes in taking recommendations from the neighboring nodes. This chapter mitigates the bad mouthing and ballot stuffing problem occurred due to false recommendation by recommender nodes up to a reasonable extent.

Chapter 7: Conclusions and Future Work: This chapter presents the conclusions and summary of the whole work. Also it deals with future research directions.