Chapter 1

Introduction

In recent years, the use of mobile ad hoc networks (MANETs) has been widespread in many applications, including some mission critical applications such as military operations, emergency situations as well as civilian ad-hoc situations like conference and classroom. In ad hoc network potential users are within the same range of radio link and participate in communication. Nodes in such networks are mobile nodes and they communicate with one another through wireless link with multi hop routing. Mobile ad hoc networks are more likely to be attacked due to lack of infrastructure and no central management. Security has become one of the major concerns in MANETs. Due to some unique characteristics of MANETs, prevention methods alone are not sufficient to make them secure; therefore, detection should be added as another defense before an attacker can breach the system.

1.1 MANETs and its vulnerabilities

Mobile ad hoc networks (MANETs) are a collection of mobile nodes that communicates over wireless media. According to Internet Engineering Task Force (IETF), MANETs is an autonomous system of mobile routers (and associated hosts) connected by wireless links; the union of which forms an arbitrary graph [25]. A set of mobile hosts carry out the basic networking functions such as routing, packet forwarding, and service discovery. It doesn’t require any pre installed infrastructure to establish the network. Nodes are self organized. These are free to move around. All the nodes in the network work as router as well as host at the same time [26][36][37]. Primary concern of the network is to maintain route traffic while connecting devices.
These are sometimes restricted to local area of wireless device or may be connected to Internet. Figure 1.1 shows a MANETs among common wireless devices. Cooperation at the network layer takes place at the level of routing by finding path for packet forwarding. Some other significant properties of MANETs are decentralization of nodes, dynamic topology and openness of media [1][2]. MANETs has emerged as an evolution of wireless technology and it is likely to be an integral part of future communication. Some areas of application of MANETs are disaster relief, battlefield communication, outdoor meeting, ubiquitous peer-to-peer market and multi-person game through Bluetooth [3]. Figure 1.2 depicts a vehicular Ad hoc Network (VANET).

Figure 1.1 Mobile Ad hoc Network (MANETs)

Figure 1.2 Vehicular Ad hoc Network (VANET)
Vulnerabilities of MANETs

Achieving security in wireless ad hoc environment is a very challenging task. Vulnerability is a weakness in security system. MANETs face a number of non-trivial challenges to the security design. MANETs is more vulnerable than wired network. Some of the vulnerabilities are as follows:

Dynamic topology: There is no fixed topology in MANETs. Nodes are free to move and can be connected dynamically in arbitrary manner. The links of network may vary over time and are based on the proximity of one node to another node.

Lack of centralized management: There is no centralized monitoring system to manage the operation of different nodes. Due to the lack of centralized monitoring system, it is difficult to detect attacks; it is not easy to monitor the traffic in a highly dynamic large scale ad hoc network.

Restricted power supply: Usually nodes in MANETs rely on battery power which is a scarce resource. Adversaries may consider it as a point to inject denial-of-service attacks. The adversary knows that the target node is battery restricted so either it can continuously send additional packets to the target or ask it for routing those additional packets or it can induce the target to be trapped in some kind of time consuming operations. By this, the battery power of target node will be drained and that may result in making the node out of service to all the genuine service requests.

Resource availability: Resource availability is a major issue in MANETs. Providing secure communication in such changing environment as well as protection against specific threats and attacks, leads to development of various security schemes and architectures. Collaborative ad-hoc environments also allow implementation of self-organized security mechanism.

Lack of Secure Boundaries: Nodes in MANETs can freely ride, join and leave the network. There is no secure boundary in MANETs. As soon as an adversary comes in the radio range of a node, it can communicate with that node due to lack of secure boundaries. MANETs are susceptible to various kinds of attacks. The attacks include
data tampering, message replay, message contamination, eavesdropping, denial of service etc.

**Scalability:** Scalability is a major issue concerning security in MANETs. Scalability can be defined as whether the network is able to provide an acceptable level of services even when large numbers of nodes are present. In MANETs due to mobility of nodes, the scale of ad hoc network keeps changing all the time.

**Cooperativeness:** Routing algorithm for MANETs usually assumes that nodes are cooperative and non-malicious. As a result, a malicious node can easily become a routing agent and disrupt network operation by disobeying the protocol specifications.

**Bandwidth constraint:** Variable low capacity links exist in MANETs as compared to wired network which are more susceptible to external noise, interference and signal attenuation effects. Wireless links have significantly lower capacity as compared to wired links.

**Adversary inside the network:** Due to lack of restricted boundary, MANETs allow the nodes to join or leave the network at any time. Thus it may contain some adversaries within the network. It is very difficult to detect such adversaries. It leads to some attack. Some of the nodes may compromise with some other nodes to attack the system.

### 1.2 Packet dropping attack: its remedies & mitigation

In ad hoc networks, a node performs both terminal function and routing functions to form an infrastructure less network. Therefore, a node becomes an integral part of the network that forwards packets towards the destination. When a node does not forward packets for others, but silently or intentionally drops them, then it is called a packet dropping attack (PDA). It is a type of denial of service in which nodes in the network drop the packets instead of forwarding. It is very challenging to detect and prevent [166][167][168], especially when the node becomes compromised due to a number of different causes. In ad hoc networks, packets may be dropped for several other
reasons in addition to genuine causes such as collisions, channel errors, buffer overflows etc.

The PDA in MANETs can be classified into several categories in terms of the strategy adopted by the malicious node to launch the attack.

Firstly, packets are dropped in the situation when a node aims on saving its own resources. This is mainly because, in a wireless environment, the most energy is consumed in the transmit mode. If a node does not forward packets, it does not use its own energy for packet transmission and preserves its energy longer.

Secondly, when a node is trying to save its bandwidth then also packets may be dropped. Bandwidth is also considered as a scarce resource in a wireless environment. To get better service for its own, it tries to save bandwidth by dropping some packets which are not meant for it. In these scenarios, it is categorized as selfish node, it can selectively drop the packets originated from or destined to certain nodes to save its own resources.

The malicious node may intentionally drop all the packets which are supposed to be forwarded. This is called a black hole attack. A special case of black hole attack dubbed gray hole attack is introduced where the malicious node retains a portion of packets (one packet out of N received packets or one packet in a certain time window), while the rest is normally relayed.

The compromised node broadcast the message [168][169] that it has the shortest path towards a destination to initiate packet dropping attack. Hence, all packet transmissions will be directed through the compromised node, and the node is able to drop the packets. If the malicious node attempts to drop all the packets, the attack can be identified through common networking tools. Moreover, when other routers notice that the compromised router is dropping all packets, they will generally begin to remove that router from their forwarding table. Hence, there is no packet transmission through the compromised node. However, it is often harder to detect the packet dropping attack, if the malicious router begins dropping packets on a specific time
period or over every $n$ packet, because some packet transmission still flows across the network.

There are certain other reasons why a node may simply drop data packets. Packets are dropped if a node malfunctions and cannot perform the regular function of forwarding packets. Such node behavior is unpredictable. When a network is congested, packets cannot be forwarded to other nodes and packets are dropped. Congestion in ad hoc networks could occur depending on ad hoc network applications.

Lastly, wireless channels are very unreliable. Burst channel errors due to interference, fading, etc. could occur while a node is sending packets over an open air interface. Like interference, when a network is jammed, data packets cannot be sent or received at any node in a jammed area. Packets from a non-jammed area cannot be sent through the jammed area and these are also dropped. Otherwise, the nodes in the jammed area don’t have any intentions to drop packets.

For malicious node mitigation, several techniques had been used. Malicious node mitigation can be classified into two categories,

(i) Prevention and protection,

(ii) Detection and response.

A prevention mechanism guards against a malicious node's attack by applying cryptographic mechanisms such as encryption and authentication. However, it cannot guard against insider attacks. A detection and response mechanism detects misbehavior activities and responds to an attack.

A protection mechanism applies cryptographic techniques to secure communications over an ad hoc network in order to prevent any malicious activity. Most research works focus on securing a routing protocol which is a key component for a wireless ad hoc network to operate properly. The two most important security services for a secure a routing protocol are authentication and data integrity services.

Many research works contribute to selfish node mitigation in ad hoc networks. It can be categorized into two approaches namely

(i) Incentive-based approaches, and
(ii) Reputation-based approaches.

An incentive-based approach aims on discouraging a node from becoming selfish. A reputation-based approach aims on detecting a selfish node and responding with appropriate action. For examples, Watchdog [161] mechanism can be used to avoid selfish node; CORE[162] is another technique which use an average weighted rating to combine direct and indirect reputations to detect and avoid selfish node. CONFIDANT [163] is another methodology through which selfish node can be detected and avoided by using weighted average rating to combine direct and indirect reputations. On detection it generates alarm to the network. TWOACK [164] avoids selfish node path.

1.3 Motivation

MANETs are vastly implemented in several areas where secure communication is mandatory. In such areas due to lack of streamline flow of data, some major problems may take place. Intermittent data flow due to malicious packet dropping may disrupt the communication between source and destination and also corrupt the entire system. Some of the typical application area of MANETs are as follows,

Military battlefield in which it is very difficult to establish infrastructure based network. For some business environments, where collaborative work is required, MANETs can play vital role. In such environment, people need to communicate amongst the group members, need secure communication. Malicious packet dropping in such scenario may disrupt the entire system. Ad-Hoc networks can autonomously link an instant and temporary multimedia network using notebook computers to spread and share information among participants at conference or classroom. Another local level application might be in home networks where devices can communicate directly to exchange information. In Personal area network and Bluetooth, MANETs are used as a short range, localized network where nodes are usually associated with a given person. Short-range MANETs such as Bluetooth can simplify the inter communication between various mobile devices such as a laptop and a mobile phone.
In commercial purpose, it can be used in emergency/rescue operations for disaster relief efforts, such as in fire, flood, or earthquake. Emergency rescue operations must take place where non-existing or damaged communications infrastructure and rapid deployment of a communication network is needed. In disaster prone area, intermittent data or malicious packet dropping in data flow may lead the system to more dangerous level.

MANETs are vulnerable to different kind of attacks [30][40]. Nodes in MANETs are susceptible to various attack which is influenced by extreme unpredictable nature of MANETs [1][29][30][32][35][38][39]. Some nodes may not cooperate for selfish and malicious reasons. Selfish nodes use system services while taking care to save some of its own resources to the extent of deviating from regular routing and forwarding. Amongst the different kind of attacks, packet dropping attack (PDA) remains a major concern. Malicious node in the network drops packets intentionally which are supposed to be forwarded to reach destination [7][8][9]. Routes that pass through such kind of nodes fail to establish path from source to destination [8]. To send the same kind of packets repeatedly, network has to consume its network resources like bandwidth, computational cost etc. a lot. It affects the entire network performance. Selfish as well as malicious nodes disrupt routing protocol and leads to reduction of network throughput, consequently network performance degrades. Previous protocols were not able to handle all type of security issues. Few protocols emerged with strong cryptographic method [33].

By considering the importance of application of MANETs and its security threat due to PDA, herein lies the motivation of development of a PDA detection methodology having capability to cope with such misbehaving nodes that involved with packet dropping attack.

At the same time, tradeoffs should be considered between the detection effectiveness and efficiency of the detection mechanism. There must be a clear analysis of different performance parameters while implementing algorithm. How does the detection technique work when malicious node deployment is very high or node mobility is
high or pause time is high. In the same network scenario, what is the performance of already existed methodology. All these analysis must be done to show the efficiency of proposed detection methodology.

1.4 Objectives

Several research efforts have been made to secure routing in MANETs [1][3][4]. Several studies that deals with security threats in MANETs [7][8][9][12][13], reveal that few of them addressed packet dropping attack in MANETs as major concern. Of course, indirectly it has been addressed. Most of the research is concerned with trusted authority to issue certificates or cryptographic authentication to routing protocol [12][13]. These methodologies are not directly concerned with network performance parameters. Dynamic nature of the network should be controlled not only by simple preventive system but also by detection system [41] that provides security to the system, without hampering normal routing as well as performance of the network. Of course routing protocol determines the ability to cop with the dynamic topology change and packet forwarding nature of the nodes. Initial protocols are not designed to withstand the malicious nodes, but subsequently different protocol extension as well as some new protocols is proposed to address the security issues of MANETs [27]. MANETs QoS such as throughput, packet delivery ratio, network overhead, end-to-end delay etc. depends on type of protocol used [31].

PDA as major concern have been addressed by [14][15][17] among others. In [14], authors proposed a mechanism to detect and isolate packet dropping attackers in MANETs, which is named as Detection and Isolation Packet Dropped Attackers in MANETs (DIPDAM). It is based on three ID messages Path Validation Message (PVM), Attacker Finder Message (AFM) and Attacker Isolation Message (AIM). It is based on End-to-End (E2E) communication between the source and the destination. This methodology is based on only single factor i.e. End-to-End (E2E) and limited to type of packets. In [15], authors proposed a distributed cooperative protocol for detecting PDA which is based cooperative participation of the nodes in a MANETs.
Here, authors utilize the redundancy of routing information to make the scheme to work in presence of transient network partitioning and Byzantine failure of nodes. But this protocol is limited to isolate the malicious nodes from the network. Moreover efficiency of this protocol has been shown only in Random walk model which is less realistic than some other mobility model like Levy walk mobility model. In [17], authors propose mechanism to monitor, detect and safely isolate the misbehaving nodes. The entire procedure is based on five different modules such as monitor, detector, isolator, investigator and witness module. But this is less tolerant with control packets which is also very crucial. Though the process overhead is less when there is no attack, yet it is high while detecting and isolating PDA. This methodology is also not concerned with collusive misbehavior where two nodes collude and conceal the dropping of each other, and node reinsertion after that is justifiable in case of temporary node failure leading to wrong isolation of benign node. Control packets misbehaving is also not handled by this methodology.

None of the methods properly address the PDA detection using collaborative/cooperative framework. The objective of this thesis is to address PDA using coalition game theoretic framework where genuine nodes will collaborate to detect PDA by neutralizing the effects of malicious nodes. Prime concern of this research is to address these issues in packet dropping attack in MANETs. We propose to address this through three different approaches:

I. **Centralized packet dropping attack detection**: In centralized packet dropping attack detection methodology, it is assumed that all data related to network communication are centrally observed. It is a static offline system. It performs statistical detection methodology. Performance of this method is compared with OCEAN (Observation-based Cooperation Enforcement in Ad hoc Networks) [173][174] an existing methodology in various network scenarios.

II. **Distributed packet dropping attack detection**: Analyzing experimental results of centralized PDA detection methodology, it is clear that this methodology is not able to handle the dynamic nature of MANETs. More complicacy may arise to the
network if it deploys malicious nodes in it. To address the distributed and dynamic nature of the problem for a network containing malicious nodes that involves packet dropping attack, distributed packet dropping attack detection methodology is proposed to detect and avoid malicious nodes from the network, based on ad hoc rules of cooperation. This methodology is named as NAODV (New Ad hoc on Demand Distance Vector). Simulation for this methodology is done for several network scenarios in Levy Walk Model of mobility and compared with two existing system namely SAODV [85][86][87][88][89][90][103][104] and TAODV [105][106].

III. Distributed packet dropping attack detection using a game theoretic approach: MANETs is formulated as coalition game in which all the genuine nodes in the network that cooperate in packet forwarding, will be in one side of the game. Malicious nodes which will try to drop the packets invariably will be in the other side of the game. Coalition is formed amongst the genuine nodes to help routing packets. Selfish nodes, as well as non responders are neither considered under the coalition of genuine node nor considered as opponents. Based on performance of the node, TRUST value of node is either increased or decreased. Accordingly a node is merged into coalition or it is splitted from the coalition. A utility function is defined which is used to measure network utility in terms of performance.

The overall scope of the research is to address the detection of packet dropping attack due to malicious node in an efficient way. Aim is to have a methodology for detection and avoidance of malicious node from the network; where the detection process should not degrade network performance parameters.

1.5 Thesis outline

The thesis is organized in six different chapters. The chapter 1 of this thesis contains introduction to MANETs. Chapter 2 contains literature reviews and general discussion of MANETs. Chapter 3 presents centralized packet dropping attack detection methodology with simulation results and comparison with OCEAN (Observation-based Cooperation Enforcement in Ad hoc Networks) [173], an existing methodology. Chapter 4 of the thesis contains distributed packet dropping attack
detection methodology with simulation results and comparative study with SAODV and TAODV. Chapter 5 presents a game theoretic approach to distributed packet dropping attack detection. Finally Chapter 6 provides research contribution, limitation of the proposed systems; also discuss possible future enhancements of current research.

Chapter 2: This chapter contains the literature review and general discussion related to different topics relevant to the proposed methodologies. It includes MANETs characteristics. It also includes different mobility models of MANETs. Security issues with respect to existing protocols are also discussed in this chapter. The chapter further contains packet dropping attack, impact of packet dropping attack and packet dropping attack detection methodologies. Then it provides concept on introduction to game theory, Game theoretic approach to detect and isolate packet dropping attack in MANETs and its equilibrium concept is also discussed.

Chapter 3: This chapter contains centralized packet dropping attack detection methodology. It describes the proposed methodology along with system model, its assumptions and different performance measurement parameters of the network. Then, it discusses the simulation environment and simulation results for various parameters and gives a comparative analysis of performance of OCEAN and proposed centralized PDA detection methodology.

Chapter 4: This chapter proposes a distributed PDA detection methodology which is named as NAODV (New Ad hoc on Demand Distance Vector). It starts with proposed system model, assumptions, different performance evaluation parameters and proposed algorithm. Thereafter simulation environment along with simulation results for various performance evaluation parameters are discussed. Simulation is also done for another two existing methodologies namely SAODV and TAODV. The chapter provides a comparative analysis and discussion of three methodologies namely NAODV, SAODV and TAODV.
Chapter 5: This chapter contains a game theoretic approach to distributed PDA detection methodology. The system model, assumptions, game strategy, utility characteristic functions and equilibrium status of proposed methodology is discussed.

Chapter 6: This chapter contains conclusion and future work. It includes research contribution of three different methodologies namely centralized PDA detection methodology, distributed PDA detection methodology and game theoretic approach to distributed PDA detection methodology. Then outlines of some of the future research directions based on the proposed methodology are provided.

The appendix of the thesis contains discussion on the network simulator i.e. NS 2, decision tree algorithm ID5R. and protocol structure for SAODV and TAODV