DETECTION OF SELFISH MISBEHAVIOR AT MAC LAYER IN WIRELESS NETWORK

A DISSERTATION

Submitted in partial fulfillment of the
requirements for the award of the degree
of

MASTER OF TECHNOLOGY
in
INFORMATION TECHNOLOGY

By

VIVEK MUSKAN

DEPARTMENT OF ELECTRONICS AND COMPUTER ENGINEERING
INDIAN INSTITUTE OF TECHNOLOGY ROORKEE
ROORKEE-247667 (INDIA)
JUNE, 2011

CANDIDATE'S DECLARATION

I hereby declare that the work, which is being presented in the dissertation entitled "**DETECTION OF SELFISH MISBEHAVIOR AT MAC LAYER IN WIRELESS NETWORK**" towards the partial fulfillment of the requirement for the award of the degree of **Master of Technology** in **Information Technology** submitted in the Department of Electronics and Computer Engineering, Indian Institute of Technology Roorkee, Roorkee, Uttarakhand (India) is an authentic record of my own work carried out during the period from July 2010 to June 2011, under the guidance of **Dr. A. K. Sarje, Professor,** Department of Electronics and Computer Engineering, IIT Roorkee.

The matter presented in this dissertation has not been submitted by me for the award of any other degree of this or any other Institute.

Date: 30-6-11

Place: Roorkee

Vivek

(VIVEK MUSKAN)

CERTIFICATE

This is to certify that the above statement made by the candidate is correct to the best of my knowledge and belief.

Date:

Place: Roorkee

30/6/2011

(Dr. A. K. Sarje)
Professor
Department of Electronics and Computer Engineering
IIT Roorkee.

ACKNOWLEDGEMENTS

First and foremost, I would like to extend my heartfelt gratitude to my guide and mentor **Dr. A. K. Sarje**, Professor, Department of Electronics and Computer Engineering, Indian Institute of Technology Roorkee, for his invaluable advices, guidance, and encouragement for sharing his broad knowledge. His wisdom, knowledge and commitment to the highest standards inspired and motivated me. He has been very generous in providing the necessary resources to carry out my research. He is an inspiring teacher, a great advisor, and most importantly a nice person.

I am thankful for the useful comments and suggestions from faculty members of our institute. I am greatly indebted to all my friends, who have graciously applied themselves to the task of helping me with ample moral supports and valuable suggestions.

On a personal note, I owe everything to the Almighty and my parents. The support which I enjoyed from my father, mother and other family members provided me the mental support I needed.

VIVEK MUSKAN

ABSTRACT

The IEEE 802.11 CSMA/CA protocol is most commonly used MAC protocol for wireless network. This protocol is used to access the media. But IEEE 802.11 works properly only if all the stations obey the MAC protocol. In public area wireless networks, it is possible that the participating hosts may deviate from the specified MAC protocol. Selfish hosts that do not obey to the MAC protocol may obtain an unfair media share. For example, IEEE 802.11 requires hosts competing for access to the channel to wait for a backoff interval, randomly selected from a specified range, before initiating a transmission. Selfish hosts may wait for smaller backoff intervals than well-behaved hosts. By this way some node can substantially increase his share of bandwidth by slightly changing the parameters of MAC protocol, in order to increase their throughput. This cause throughput degradation of all well behaved node.

In this dissertation, we proposed the detection scheme for selfish misbehavior at MAC layer in wireless networks based on comparative study of Throughput, RTS retransmission rate and packet retransmission rate of nodes under well behaved and selfish attack.

Table of contents

Page No.

LIST OF FIGURES

Figure No. **Page No.**

LIST OF TABLES

Table No. **Page No.**

Chapter 1

Introduction

1.1 Introduction and Motivation

Reliable communication in wireless networks depends on inherent trust among nodes. Trust means that nodes need to fully cooperate with each other to ensure correct route establishment mechanisms, protection of routing information and security of packet forwarding. The IEEE 802.11 distributed coordination function (DCF) mode combines carrier sensing with collision avoidance and is considered the most popular MAC access protocol for wireless networks. IEEE 802.11 is designed under the assumption of a friendly and cooperative environment. However, due to the open nature of the wireless medium, the pervasiveness of wireless devices, and the ease of configuration, the network becomes more vulnerable to security attacks, especially in the presence of hostile hosts.

The distributed operation of 802.11 DCF and the lack of a fully trusted centralized authority make wireless networks significantly vulnerable to attacks. In addition, the wireless medium is inherently error-prone with limited channel capacity. A node that fails to adhere to the specifications might be caused by either violation of the proper operation of the protocol (misbehavior) or other normal behavior, such as channel errors, collisions, interference, and hidden terminals. Alternatively, the increasing volume of networking protocols requires a flexible and simplified way to perform easy reconfiguration and deployment for users with average expertise. The rising trend to implement standard protocols in software and firmware has led to an extreme where wireless network adapter and devices have become easily programmable. Consequently, it becomes practically feasible for a network peer to tamper with software and firmware, and modify its wireless interface and default parameters, thus ultimately forcing the protocol to deviate from normal behavior. The objective, however, may vary from a selfish user cheating to obtain better access to the valuable wireless resources (e.g., bandwidth) to a malicious user attempting to destroy network services (e.g. denial of service [DoS]).

The IEEE 802.11 is a standard for a wireless LAN covering both physical and MAC layers. The IEEE 802.11 MAC protocol provides two service types of service: asynchronous and synchronous (or, rather, contention free).

The asynchronous type of service is provided by the Distributed Coordination Function (DCF) which implements the basic access method of the IEEE 802.11 MAC protocol and is also known as the Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) protocol. This IEEE 802.11 CSMA/CA [13] protocol is used for sharing the wireless channel among the various nodes.

The contention resolution mechanism depends on inherent trust among nodes. In environments where hosts in the network are untrusted, some hosts may misbehave by failing to adhere to the network protocols, with the intent of obtaining an unfair share of the channel.

In such an environment, by simply manipulating the back-off timers and/or wait times prior to transmission, selfish nodes can cause a drastically reduced allocation of bandwidth to well behaved nodes. So it is necessary to detect selfish misbehavior in wireless network.

1.1 Statement of the Problem

The wireless network is vulnerable to various kinds of attacks. When dealing with MAC layer, there are two type of misbehavior: selfish misbehavior and malice misbehavior. In this work, we focus on the selfish misbehavior.

The aim of this dissertation is to detect the selfish misbehavior at MAC layer in wireless network. In the selfish misbehavior detection scheme we first of all collect the statistical values of all wireless nodes RTS retransmission due to time out, packet retransmission due to ACK timeout and throughput at receiver end then compare it with the threshold value.

1.2 Organization of the Report

This dissertation report comprises of six chapters including this chapter that introduces the topic and states the problem. The rest of the report is organized as follows.

Chapter 2 gives the background of IEEE 802.11 WLAN, working of MAC protocol and literature review of misbehavior detection techniques and types of misbehavior in wireless network. It also includes the research gaps found.

Chapter 3 gives the proposed framework for detection of selfish misbehavior in wireless network.

Chapter 4 gives the description of simulation environment used and the simulation topology and simulation metrics.

Chapter 5 discusses the experimental results, validation of the detection scheme and analysis of the result.

Chapter 6 concludes the dissertation work and gives scope for future work.

Control (DLC) layers.802.11x defines both PHY and DLC layers except LLC sub layer. LLC is same for all 802.11 family. As indicated in Fig.2.1, DLC is subdivided into Medium Access Control (MAC) and Logical Link Control (LLC) sub layers. Whereas, PHY is subdivided into Physical Medium Dependent (PMD) and Physical Layer Convergence Procedure (PLCP) sub layers.

PMD is the lowest sub layer and close to the air-interface, which is responsible for sending and receiving data via wireless channel and defines the transmission scheme. PLCP sub layer adapts and maps MAC request, which is common for different PHYs, into a format specific to the applied PMD. The main difference between 802.11 (a) and (b) is in the PHY layer. 802.11a supports 8 different PHY modes based on OFDM in 5 GHz-UNII band, whereas, 802.11b supports 3 PHY modes based on Frequency Hopping Spread Spectrum (FHSS), Direct Sequence Spread Spectrum (DSSS) in 2.4 GHz-ISM band. A brief description of IEEE 802.11 family is discussed later.

2.1.2 Network architecture

In a service arrangement where the participating wireless stations can independently communicate to each other, is called Independent Basic Service Set (IBSS) prior to each of them has the ability to initiate and establish such connection. This peer-to-peer connected network is also called Ad Hoc network, which is independent of Access Point (AP) as illustrated in Fig. 2.2. Coordination of channel accessing is distributed among the participating stations.

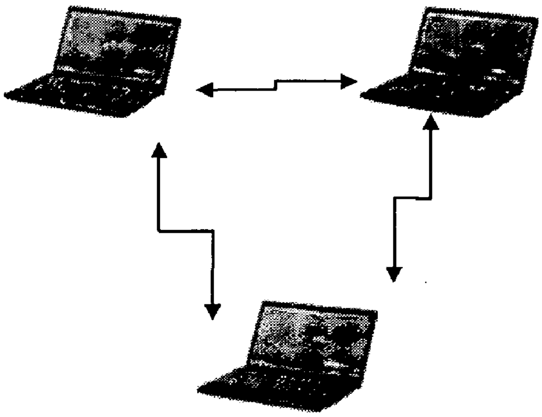

Figure 2.2: Independent BSS

Wireless stations are always connected with an AP to receive service in an Infrastructure based BSS as in today's mobile communication system. In this case, user equipments or wireless stations cannot communicate directly to each other, rather through the AP. BSS defines both independent and infrastructure based basic service set. In a system where more than one such BSS included, is called Extended Service Set (ESS), which is similar to a multicell system. Fig. 2.3 illustrates an ESS, which is formed by two Infrastructure based BSSs and connected by Distributed System (DS).

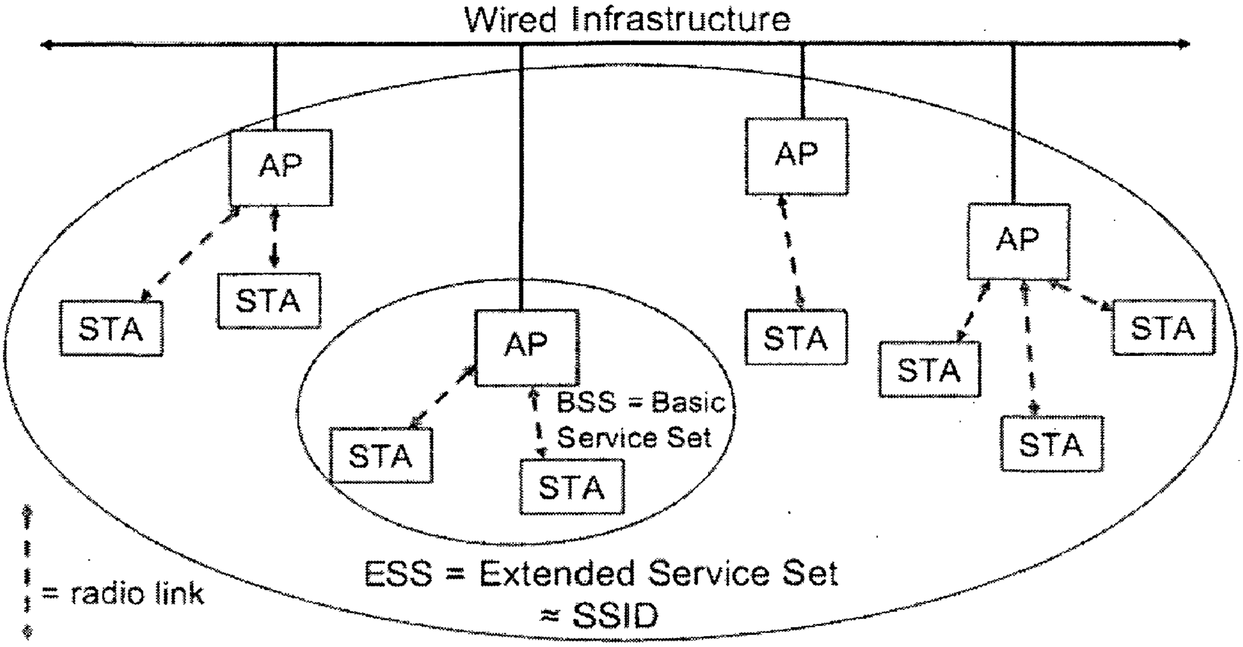

Figure 2.3: Infrastructure based BSS

2.2 Carrier sensing for collision avoidance

CSMA/CA multi-access protocol is used in 802.11a for sensing the medium and acquire the access if a station (contending player: in terms of game theory) finds the intended channel free of any transmission. Otherwise, CSMA scheme defers as to when the transmission is tried again. In 802.11 MAC [13], two types of carrier sensing are defined: mandatory physical carrier sensing and optional virtual carrier sensing. Physical carrier sensing monitors the RF energy level in the air to detect any possible ongoing transmission while virtual carrier sensing uses handshaking mode request-to-send (RTS)/ clear-to-send (CTS) to ensure that the air medium is reserved prior to transmitting data frame. By RTS frame a transmitter informs other stations in range and by CTS a receiver informs in range about the anticipated transmission to avoid any collision. Both RTS and CTS frames contain the information of how long it does take to transmit the next data frame, which instructs the neighboring stations to reset their Network Allocation Vector (NAV) timer.

In wireless medium access, unlike wire-line environment, collision detection is not feasible because of duplex communication, capable of receiving and transmitting simultaneously, which would increase the price of the mobile device. Also for detection, all participating stations need to hear each other and practically it is impossible to hear at the receiver end in wireless environment. Carrier sense attempts to avoid collisions by testing the signal strength (RSSI) in the vicinity of the transmitter. However, collisions occur at the receiver not at the transmitter, indicating the presence of two or more interfering signals at the receiver that constitutes a collision. Since the receiver and the sender are typically not collocated, carrier sense does not provide the appropriate information for collision avoidance.

2.2.1 Hidden and exposed terminal problem

Referring to the discussion of the previous paragraph, two possible difficulties are. common with CSMA/CA: hidden station and exposed station. In Fig. A.4, there is an illustration of these two problems. B is in the range of both A and C. When A transmits to B (where B is the receiver) C does not know about the transmission since it is out of the range of A. Therefore, if C (hidden terminal) also transmits intending to B, there will be a collision at B.

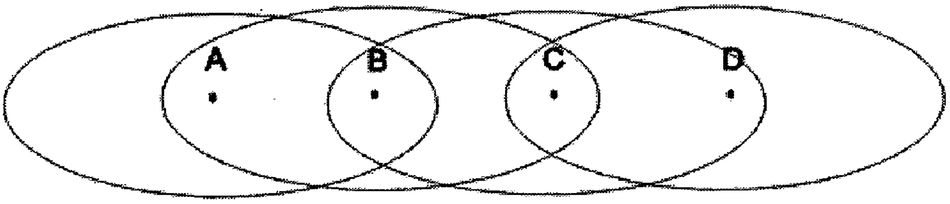

Figure 2.4: Hidden terminal problem

On the other hand, if B transmits to A (receiver), C defers sensing the channel is busy. At this time if D (out of range of B) likes to transmit to C, it will not hear from C because of deferring status. However, there is no reason to defer transmission to a station other than B. This problem is called as exposed terminal problem. Carrier sense provides information about potential collisions at the sender but not at the receiver. This information can be misleading when the configuration is distributed so that not all stations are within range of each other.

In an overlapping scenario of multiple coexisting BSS, hidden terminal problem may be a reason of neighborhood capture effect. Terminals not knowing each other's existence can occupy the channel for a longer time, while the other terminals within the detecting range and following LBT (listen-before-transmit) wait until the channel becomes available. This uncoordinated activity can reduce the affected terminals' throughput dramatically by increasing delay. The virtual carrier sensing can minimize (if not resolve completely) these two problems.

2.3 MAC protocol:

The IEEE 802.11 MAC protocol provides two service types: asynchronous and synchronous (or, rather, contention free). These types of services can be provided on top of a variety of physical layers and for different data rates. The asynchronous type of service is always available whereas the contention free is optional. The asynchronous type of service is provided by the Distributed Coordination Function (DCF) which implements the basic access method of the IEEE 802.11 MAC protocol and is also known as the Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) protocol. The contention free service is provided by the Point Coordination Function (PCF) which basically implements a polling access method. The PCF uses a Point Coordinator, usually the Access Point, which cyclically polls stations giving them the opportunity to transmit. Unlike the DCF, the implementation of the PCF is not mandatory. Furthermore, the PCF itself relies on the asynchronous service provided by the DCF.

2.3.1 Point Coordination Function (PCF):

To provide time-bounded service, the standard specifies a point coordination function (PCF) on top of the standard DCF mechanisms. It Support for time-bounded data such as voice or video. As opposed to DCF, where control is distributed to all stations, in PCF mode a single AP controls access to the media. If a BSS is set up with PCF enabled, time is spliced between the systems in PCF mode and DCF (CSMA/CA) mode. AP will poll each station for data, and after a given time move on to the next station. No station is allowed to transmit unless it is polled; and stations receive data from AP only when they are polled. During PCF period a maximum latency is guaranteed. AP needs to have control of media access and must poll all stations, which could be ineffective in large network.

2.3.2 Distributed coordination function:-

According to the DCF a station must sense the medium before initiating the transmission of a packet. If the medium is sensed as being idle for a time interval greater than a Distributed InterFrame Space (DIFS) then the station transmits the packets. Otherwise, the transmission is deferred and the backoff process is started. Specifically, the station computes a random time interval, the backoff interval, uniformly distributed between zero and a maximum called Contention Window (CW). This backoff interval is then used to initialize the backoff timer. This timer is decreased only when the medium is idle, whereas it is frozen when another station is transmitting. Specifically, each time the medium becomes idle, the station waits for a DIFS and then periodically decrements the backoff timer. The decrement period is referred to as the slot-time which corresponds to the maximum round-trip delay within the BSS and, hence, depends on the maximum BSS coverage.

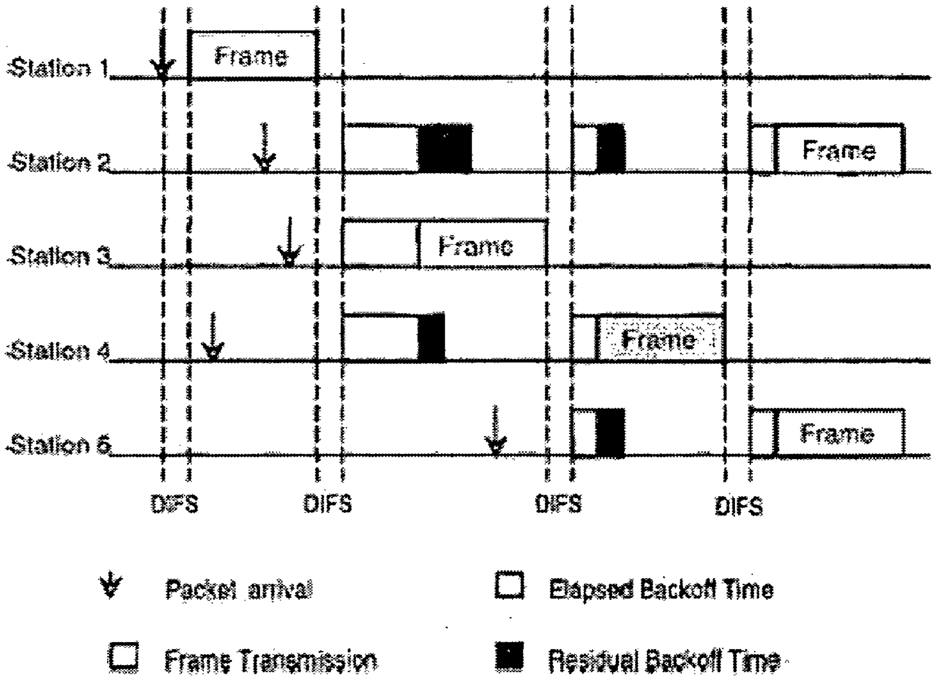

Figure 2.5: Basic access mechanism

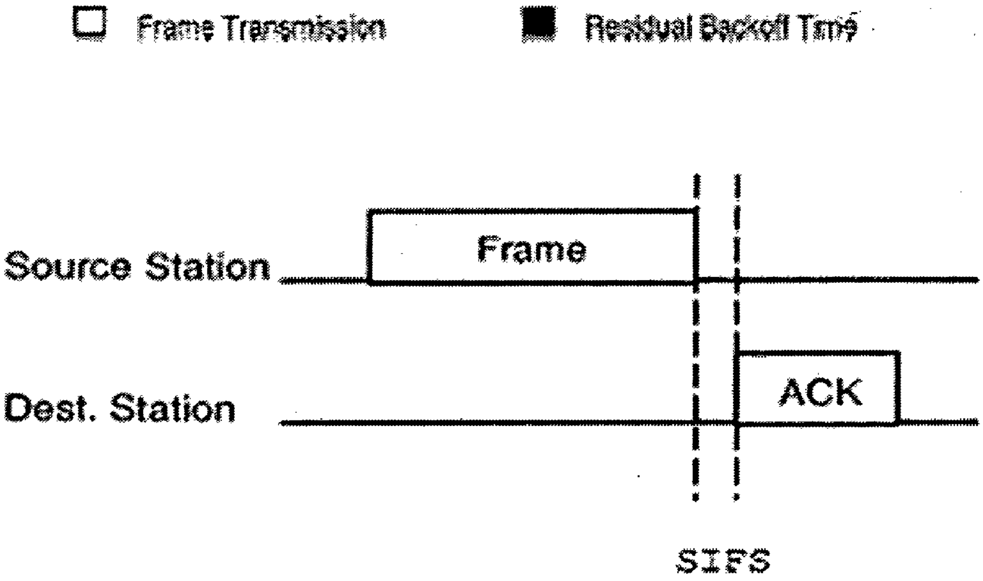

Figure 2.6:- Acknowledgment mechanism.

As soon as the backoff timer expires, the station is authorized to access the medium. Obviously, a collision occurs if two or more stations start transmission simultaneously. Unlike wired networks (e.g., with CSMA/CD), in a wireless environment collision detection is not possible. Hence, as shown in figure 2.3, a positive acknowledgment is used to notify the sending station that the transmitted frame has been successfully received. The transmission of the acknowledgment is initiated at a time interval equal to the Short InterFrame Space (SIFS) after the end of the reception of the previous frame. Since the SIFS is, by definition, less than the DIFS1 the receiving station does not need to sense the medium before transmitting the acknowledgment. If the acknowledgment is not received the station assumes that the transmitted frame was not successfully received and, hence, schedules a retransmission and enters 1 The DIFS is defined as DIFS = SIFS + 2 Slot- times. The backoff process again. However, to reduce the probability of collisions, after each unsuccessful transmission attempt, the Contention Window is doubled until a predefined maximum (CWmax) is reached. After a (successful or unsuccessful) frame transmission, if the station still has frames queued for transmission; it must execute a new backoff process. In radio systems based on medium sensing, a phenomenon known as the hidden station problem may occur. This problem arises when a station is able to successfully receive frames from two different transmitters but the two transmitters cannot receive signals from each other. In this case a transmitter may sense the medium as being idle even if the other one is transmitting. This results in a collision at the receiving station. To deal with the hidden station problem, the IEEE 802.11 MAC protocol includes an optional mechanism which is based on the exchange of two short control frames given in [2]. Furthermore, the RTS/CTS mechanism can be regarded as a way to improve the MAC protocol performance. In fact, when the mechanism is enabled, collisions can obviously occur only during the transmission of the RTS frame. Since, the RTS frame is usually shorter than the data frame the wastage in bandwidth and time due to the collision is reduced. In both cases the effectiveness of the RTS/CTS mechanism depends upon the length of the data frame to be protected. It is reasonable to think that the RTS/CTS mechanism improves the performances when data frame sizes are large when compared to the size of the RTS frame. Consequently, the RTS/CTS mechanism relies on a threshold, the RTS threshold.

2.3.3 DCF timing relations

As mentioned earlier that a station needs to monitor the channel for a minimum time interval called Distributed Inter Frame Space, DIFS. Hence, the total time she needs to monitor the channel is the random backoff time (based on incremental CW) on top of DIFS for each attempt. There are four types of prioritized time interval: Short Inter Frame Space (SIFS), PCF IFS (PIFS), Distributed IFS (DIFS) and Extended IFS (EIFS). In an ongoing transmission, when a station sends a frame she waits the shortest time interval SIFS to receive an ACK (a token of successful reception) in the next SIFS and continues to send the frame-stream. If there is no ACK in the next SIFS, after waiting an EIFS she again starts random backoff to contend for the channel. PIFS is the second prioritized time interval, which is centrally controlled by APs to pick a node giving her higher priority over other nodes contending by DIFS. Fig. 2.4 illustrates the DCF channel access and comparative timing.

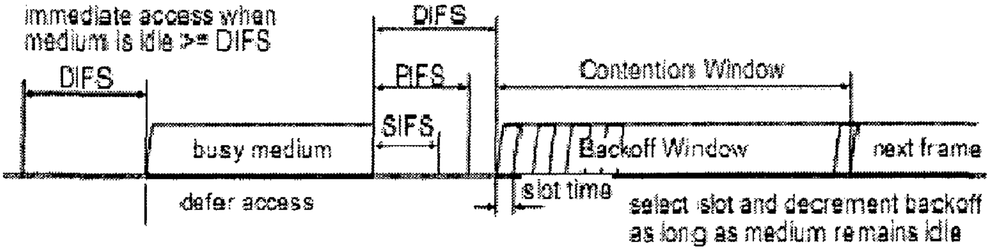

Figure 2.7: IEEE 802.11 DCF channel access [13]

2.4 MAC frame format

Beside data frame, there are two types of MPDU frames in 802.11: control frames (ACK, RTS, CTS), management frames (beacon, association, authentication). In this thesis, we consider DCF basic access mode, which includes data and acknowledge (ACK) frames, as illustrated in Fig. A.9. There is four addresses in the MAC header of the data frame: destination address (DA, addr1), source address (SA, address 2), transmitting station address (TA, address 3), receiving station address (RA, address 4). DA identifies the final recipient(s) of the MPDU, SA identifies the source station from where the MPDU is initiated, TA identifies the station currently transmitting and RA is the immediate recipient station in the wireless channel. However, RA is used only for the wireless AP-to-AP communication, which is not common [15]. FCS contains a 32-bit cyclic redundancy check (CRC) value, which is created by the sending MAC and is recalculated by the receiving MAC to check for damaged frames. Final data frame MPDU length depends on the variable payload size (max. 2304 or 2312 with WEP) on top of 30-byte MAC header and 4-byte FCS. In contrast with data frame, ACK frame contains only one address (RA) and excludes payload. Therefore, ACK is a fixed size MPDU with 12-byte length.

MAC header

Frame control	Dur. /ID	Address1 (DA)	Address2 (SA)	Address3 (TA)	Sequence control	Address4 (RA)	Frame body	FCS
Bytes2	2	6	6	6	2	6	0-2304	4

data frame

MAC header

Frame control	Dur./ID	RA	FCS
Bytes 2	2	6	4

Control frame

Figure 2.8: MAC frame format[13]

2.5 Selfish Misbehavior

The successful operation of wireless network is totally dependent on the cooperation of participating nodes in communication. The lack of a fixed infrastructure in ad hoc networks forces ad hoc hosts to rely on each other in order to maintain network stability and functionality. But sometimes nodes do not work as they are intended due to conservation of their resources such as energy, memory, and bandwidth. Such nodes are called misbehaving nodes or non cooperative nodes and are of following types:

Malicious Node: Nodes that perform active attacks with the aim of damaging other nodes by causing network outage are considered to be malicious [21], also referred to as compromised nodes. In addition, a compromised node may use the routing protocol to advertise itself as having the shortest path to the node whose packets it wants to intercept as in the so called black hole attack.

Selfish Node: Selfish nodes [21] work in a wireless network for their own benefit. They simply do not forward packets (data packets and/or control packets) of other nodes to conserve their own energy, or push their own packets in front of the buffer queue. Selfish nodes disturb the performance of wireless network to a great extent. When a node becomes selfish it does not cooperate in data transmission process and causes a serious affect on network performance. We have performed simulation analysis of node misbehavior only with selfish node.

As observed in [23], misbehavior can occur under the various protocol stacks of the OSI layer namely the MAC-layer, the network layer, the transport layer and lastly the middleware/application layer. For the sake of completeness, the various deviating misbehavior will be described briefly. The various manners in which nodes can resist cooperation under the respective protocol stacks are as follows:

2.6 Misbehavior at different layer:

2.6.1 MAC Layer: The current de facto MAC standard for wireless network is the IEEE 802.11 protocol. It is based on a fully distributed mechanism called the

Distributed Co-ordination Function (DCF) that aims to prevent unfair channel utilization and resolve contention among the different nodes. After a transmission session, all nodes are required to select a backoff value from a preset range to begin their backoff session which serves to enforce the principle that no nodes can transmit consecutively to ensure fairness in the long run. Deviating nodes can thus circumvent this mechanism in two ways: (i) selecting smaller backoff values, not using those that is specified by the protocol; (ii) using a totally different retransmission strategy.

IEEE 802.11 MAC protocol favors the node that selects the smallest back-off value among a set of contending nodes. Therefore, a selfish node may choose not to comply with protocol rules by selecting small back-off intervals to gain significant advantage in channel sharing over well-behaved nodes. Moreover, due to the exponential increase of the contention window after each unsuccessful transmission, well-behaved nodes will select their backoff value from larger intervals after every collision. Therefore, the chance of their accessing the channel becomes even smaller. Apart from intentional selection of small back-off values, a node can deviate from the MAC protocol in other ways as well. It can choose a smaller contention window or he may wait for an interval shorter than DIFS(Distributed inter frame space), or reserve the channel for an interval larger than the maximum allowed NAV (Network Allocation Vector) duration.

A misbehaving host may obtain more than its fair share of the bandwidth by:

- Selecting backoff values from a different distribution with smaller average backoff value, than the distribution specified by DCF (e.g., by always selecting a fixed backoff of 1 slot).
- Using a different retransmission strategy that does not double the CW(congestion window) value after collision.

2.6.2 Network layer

- **Rushing attacks**: Rushing attacks targeting the on-demand routing protocols were amongst the first exposed attacks on the network layer of multi-hop route failures or changes can seriously disrupt the normal functioning of TCP. Packets dropped at intermediate nodes because of route changes will wrongly be misinterpreted as congestion problems by TCP. They can also cause frequent out-of-order delivery, exacerbating the problem. Although current proposed solutions call for intermediate nodes to inform the sender of route failures, such schemes would be useless if the intermediate node happens to be a misbehaving entity. The sender would then assume the lack of acknowledgments to be a sign of congestion.

2.6.4 Middleware/Application Layer: Cooperation at this end has not been fully investigated since full scale commercial MANET is not in widespread use yet. However, given that the nature of these applications fits the wired P2P paradigm, it is expected that they inherit problems typical of P2P systems such as not sharing their file repositories to the entire community.

2.7 The 802.11 standards

The IEEE 802.11: The root standard defines operation and interfaces at MAC and PHY layers for wireless LAN. Three different PHY interfaces are defined: one is based on Infra Red (IR) and other two are based on Frequency Hopping Spread Spectrum (FHSS) and Direct Sequence Spread Spectrum (DSSS). The latter two use 2.4 GHz unlicensed Industrial Scientific and Medical (ISM) band.

IEEE 802.11a: This extension defines the PHY, which supports up to 54 Mbps data rate based on Orthogonal Frequency Division Multiplexing (OFDM) in 5 GHz Unlicensed National Information Infrastructure (UNII) band similar to European Hiper LAN/2.

IEEE 802.11b This extension is a supplement of 802.11 standard providing high speed PHY layer in 2.4 GHz ISM band and supports up to 11 Mbps data rate. The higher data rate is achieved by 8-chip Complementary Code Keying (CCK) modulation scheme. This is also known as Wireless Fidelity (Wi-Fi).

IEEE 802.11c This is not an extension but a task group providing information for changes and modification in other standards. The 802.11c task group defined AP bridging protocol.

IEEE 802.11d This standard defines the radio regulatory domains. Frequency spectrum regulation defers from nation to nation, therefore, a station gets associated with a network only if it complies with the specific regulatory domain.

IEEE 802.11e Similar to 802.11c, this is a task group defining enhancements to 802.11 to allow Quality of Service (QoS) support, which works with any PHY extension.

IEEE 802.11f It defines the intercellular mobility with different vendors and supported by Inter AP Protocol (IAPP).

IEEE 802.11g This extension enhances the popular rolled-out 802.11b with higher throughput similar to 802.11a i.e. 54 Mbps based on OFDM transmission scheme in 2.4 GHz band. Another data rate 33Mbps, is also supported by PHY based on DSSS, therefore, coexistence with 802.11b is possible that makes 802.11g more attractive.

IEEE 802.11h This group is tasked to define the Transmit Power Control (TPC) and Dynamic Frequency Selection (DFS) issues.

IEEE 802.11i This task group defines the security and privacy issues by Wired Equivalent Privacy (WEP), Wireless Protected Access (WPA) and Advanced Encryption Standard (AES) protocols.

2.8 Literature Review

Many selfish misbehavior detection approaches are proposed for detecting selfish behavior in network traffic but selfish or greedy behavior of nodes at MAC layer remains a hard to resolve problem. The proposed methods regarding detection of MAC layer misbehavior in wireless networks are as follows:

Kyasanur and Vaidya [2] have addressed the MAC layer misbehavior using detection and correction mechanisms. In this detection method, the receiver assigns and sends backoff values to the sender in CTS and ACK frame and uses this information to detect potential misbehavior. In case of misbehavior, the receiver penalizes the sender by increasing its backoff values for the next transmissions. It gives control to the receiver over the sender, by making the receiver assign backoff values to the sender in both the detection and the correction schemes. It also requires a modification of the IEEE 802.11 MAC protocol.

Raya and Hubaux [4] uses a detection system that does not require any modification to the MAC protocol. The system is implemented at the access point (AP), and the AP is assumed to be trusted. Traffic traces of sending hosts are collected periodically during short intervals of time called monitoring periods. This gathered data is then passed to six tests within the DOMINO algorithm. Each of these tests corresponds to a designated misbehavior (e.g. backoff manipulation, oversized NAV). The result of each test is then fed into a decision making component, which in turn will infer whether a particular station is misbehaving or not, and a certain reaction scheme (i.e., deny traffic from cheaters) will be invoked thereafter. A node misbehaves when its corresponding cheat counter exceeds a certain threshold (i.e., to reduce false positives). Misbehaving nodes are then punished using a punishing function. DOMINO fails to detect an adaptive cheater which alternate randomly among several misbehavior techniques in order to evade detection. Guang ans Assi [11] presented a Predictable Random Backoff (PRB). It is based on minor modifications of the 802.11 Binary Exponential Backoff (BEB) and forces each node to generate a predictable backoff interval; the key idea is to adjust, in a predictable manner, the lower bound of the contention window in order to enhance the per-station fairness in selfish environments. Hosts that do not follow the operation of PRB are therefore easily detected and isolated.

A related approach is to design protocols which are resilient to misbehavior. In the context of TCP, Savage et al. [16, 17] identify certain receiver misbehavior that may allow a misbehaving receiver to gain a throughput advantage over other well-behaved receivers, by exploiting weaknesses in the TCP congestion control algorithm used by the sender. Savage et al. propose simple modifications to TCP, which prevent a misbehaving receiver from gaining significant throughput advantage.

Game-theoretic techniques have been used to develop protocols which are resilient to misbehavior. Game-theoretic approach assumes that all users are selfish and rational. Rational hosts always select a strategy that maximizes their utility (utility is a measure of the benefit obtained by a host). Protocols are designed that reach an equilibrium state called the "Nash equilibrium", where a selfish host cannot gain any advantage over well-behaved hosts. Game-theoretic approaches are well suited for designing protocols resilient to selfish misbehavior, and we discuss in detail below, some representative work.

Michiardi et al. [12] study mechanisms to address selfish misbehavior at the routing layer. They model the hosts in the network as participants in a non-cooperative game with each host attempting to maximize its own utility. By imposing suitable costs on each network operation such as packet forwarding, the game reaches Nash equilibrium. In practice, selecting the right cost for each operation is hard. In addition, a pricing infrastructure must be available to ensure hosts pay for the services that they obtain.

Mackenzie et al. [18] consider selfish misbehavior in Aloha protocol. Hosts are assumed to incur a cost for each transmission (e.g., energy required for the transmission), and each host is assumed to have perfect knowledge of channel conditions and backlogged hosts (in practice, this knowledge may not be available to hosts in the network). Under this setting, it is shown that the protocol has Nash equilibrium. When all hosts follow the strategy proposed by Mackenzie et al., there is no scope for selfish misbehavior.

Konorski [19] studies selfish MAC layer misbehavior, where hosts deviate from the specified backoff strategy. Konorski proposes a modified backoff algorithm using black-bursts, and with a game-theoretic analysis shows that the protocol is resilient to selfish misbehavior. Konorski's work assumes that all hosts can accurately measure the duration and originator of each black-burst, which is hard to guarantee in a wireless network.

Most of the protocols using game-theoretic techniques are based on the assumption of Perfect Information", i.e., every host can observe all the actions of other hosts in the network. This assumption is hard to realize in practice, especially in the context of a wireless network (with fading channels, hidden terminals, etc.). In addition, protocols developed with game-theoretic techniques may not achieve the performance of protocols developed under the assumption that all hosts are well-behaved and cooperate with each other (e.g., IEEE 802.11).

Intrusion detection and tolerance techniques are used as tools for diagnosing and tolerating misbehavior [20]. Intrusion detection approaches are based on developing a long-term profile of normal activities, and identify intrusion by observing deviations from the long-term profile.

2.9 Research Gaps

Many selfish misbehavior detection approaches are proposed for detecting selfish behavior in network traffic but selfish or greedy behavior of nodes at MAC layer remains a hard to resolve this problem. Some of the flaws in these schemes are:

Kyasanur [2] requires a modification of the IEEE 802.11 MAC protocol in a way that is incompatible with the current standard. Such an approach is practically unfeasible. Because it creates communication and computation overhead. The first is due to the addition of new frame header fields and the second to the detection and correction schemes that have to compute backoff and, in some cases, penalties for each individual frame of the sending station (in the infrastructure case, all this load will be centralized at the AP).

Mitchell [7] gives control to the receiver over the sender, by making the former assign backoff values to the latter in both the detection and the correction schemes. Hence the proposed approach opens the door to new misbehavior techniques, including misbehaving receiver and collusion between sender and receiver.

DOMINO [4] fails to detect an adaptive cheater which alternates randomly among several misbehavior techniques in order to evade detection.

Konorski [5] considers an ad hoc network in which all stations hear each other and he proposes a misbehavior-resilient backoff algorithm based on game theory. As it requires a new backoff mechanism, different from the current standard, this solution is not practical for current hotspots.

In [10] a new class of protocol-compliant attacks, timeout attack, has been presented to disrupt packet forwarding, thereby defeating a Watchdog-like detection system deployed at the MAC layer. This type of attack can deliberately delay the transmission of MAC frames, such as RTS and DATA, by a minimum required time. Consequently, a malicious node can force a well behaved node to drop the packets at the MAC layer while the malicious node itself completely follows the protocols, thus hiding from the Watchdog detection system.

The common disadvantage of the herein described solutions is that either, it requires a modification of IEEE 802.11 MAC protocol or, it creates communication and computation overhead. So this type of approach is practically unfeasible.

Chapter 3

Proposed Framework

The proposed framework is designed to detect selfish MAC misbehavior in wireless network, where the host is using IEEE 802.11 DCF mode. The goal of detection scheme is to simplify misbehavior detection.

We use the mean of a sample of n observations to detect the deviation from normal behavior. In case of throughput, if the mean of sample of n observation is smaller than the threshold then it may be the sign of selfish misbehavior in wireless network. In case of packet delivery ratio and RTS retransmission, if the mean of sample of n observation is greater than the threshold then it may be the sign of selfish misbehavior in wireless network. We set the threshold to (expected mean-0.1×max), where max is the expected maximum of all generated numbers.

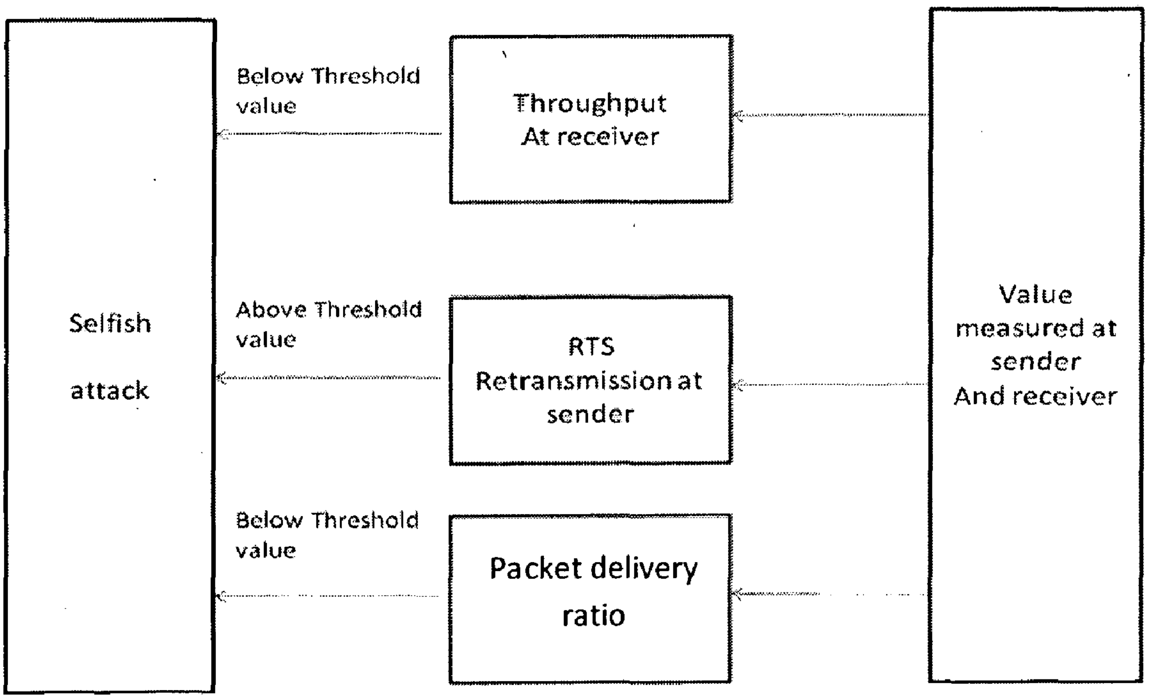

Figure 3.1 Detection scheme

Throughput at receiver: it is the average rate of successful message delivery over a communication channel.we calculate the mean of throuhput in the network when there is no misbehaving node in the network. This mean of throughput is said to be expected mean of the throughput. Then the threshold value is calculated by the formula:

Threshold= expected mean-0.1×max

Where max= maximum of throughput in n number of observations.

In the presence of selfish node, first of all collect the statistical values of throughput at receiver end then compare it with the threshold value.

If it is below threshold then selfish attack is occurring otherwise scenario is not containing any selfish nodes all are working properly without any selfishness.

Packet delivery ratio: Packet Delivery Ratio (PDR) is the ratio of total number of packets sends to total number of packets received. Expected mean of packet delivery ratio is caculated in same way like the expected value of throughput.

In the presence of selfish node, first of all collect the statistical values of Packet Delivery Ratio at receiver end then compare it with the threshold value.

If it is below threshold then selfish attack is occurring otherwise scenario is not containing any selfish nodes all are working properly without any selfishness.

RTS retransmission at sender: In case of misbehavior channel gets busy and there is more collision, so the RTS retransmission at sender increases.

Expected mean of RTS retransmission at sender is caculated in same way like the expected value of throughput. In the presence of selfish node, first of all collect the statistical values of RTS retransmission at sender end then compare it with the threshold value.

If it is above threshold value then selfish attack is occurring otherwise scenario is not containing any selfish nodes all are working properly without any selfishness

Chapter 4
Simulation environment

This chapter provides a short overview on the simulation model.

4.1 Introduction

Simulation is a fundamental tool in the development of wireless network protocols, because the difficulty to deploy and debug them in real networks. The simulation eases the analyzing and the verification of the protocols, mainly in large-scale systems. It offers flexible testing with different topologies, mobility patterns, and several physical and link-layer protocols. However, a simulation cannot provide evidence in real-world scenarios, due to assumptions and simplifications that it makes. Various examinations, such as [60], show significant divergences between different simulators that demonstrate an identical protocol. Therefore, the results obtained from the simulations should be evaluated appropriately.

- Three well-known simulators are used for wireless network simulations: NS-3, GloMoSim and OPNET. We chose NS3 [14], because it is a scalable simulator that allows to study Internet protocols and large-scale systems in a controlled environment.

NS-3 overview

- NS-3 is a discrete-event network simulator for Internet systems.
- NS-3 allows researchers to study Internet protocols and large-scale systems in a controlled environment.
- NS-3 is a new simulator (not backwards-compatible with ns-2)
- NS-3 is a free, open source software project organized around research community development and maintenance.

Layer	Model
Support	Random number generator, tracing, monitors, error models
Physical layer	Two way shadowing, Energy model, Satellite repeater, 802.11a, basic wired loss and delay
Link layer	ARP, HDLC, Queuing: Drop tail, MACs: CSMA, 802.11b, WPAN, satellite aloha, point to point, 802.11 MAC low and high and rate control algorithm.
Network layer	IP, mobile IP, generic distance vector link state, IPv4,global static routing, AODV, DSR, DSDV, OLSR
Transport layer	TCP(many variant), UDP, SCTP, TFRC, RAP,UDP
Application layer	Ping, telnet, FTP, HTTP, socket API

Table 4.1: NS3 overview

The layers are separated and each layer has its own API. The layers interact with each other using message-passing approach. A combination of different protocols at various layers into a complete protocol suite, as well as extension with alternative protocols, can be done simply.

4.2 Simulation topology and simulation metrics

Various network scenarios were analyzed to prove the model's correctness and characteristics. Every plot was taken as an average of ten different runs. In the simulation experiment; we tested networks from 8 up to 50 mobile hosts. The nodes were placed randomly in the area of 1500m*750m to maintain the network density and connectivity as constant and balanced. In all the simulations, we used standard parameters of the channel and radio model: channel capacity of 2MB/s, free space propagation model and radio propagation range of 250 meters. The IEEE 802.11 protocol was used as the medium access control protocol.

The traffic was produced using a traffic generator, which made randomly constant bit rate (CBR) sessions. The data packet size was 512 Bytes and no fragmentation was used. The channel bit rate is 2 Mbps. The simulation time for each run is 25seconds. The results are averaged over 10 runs of the simulation.

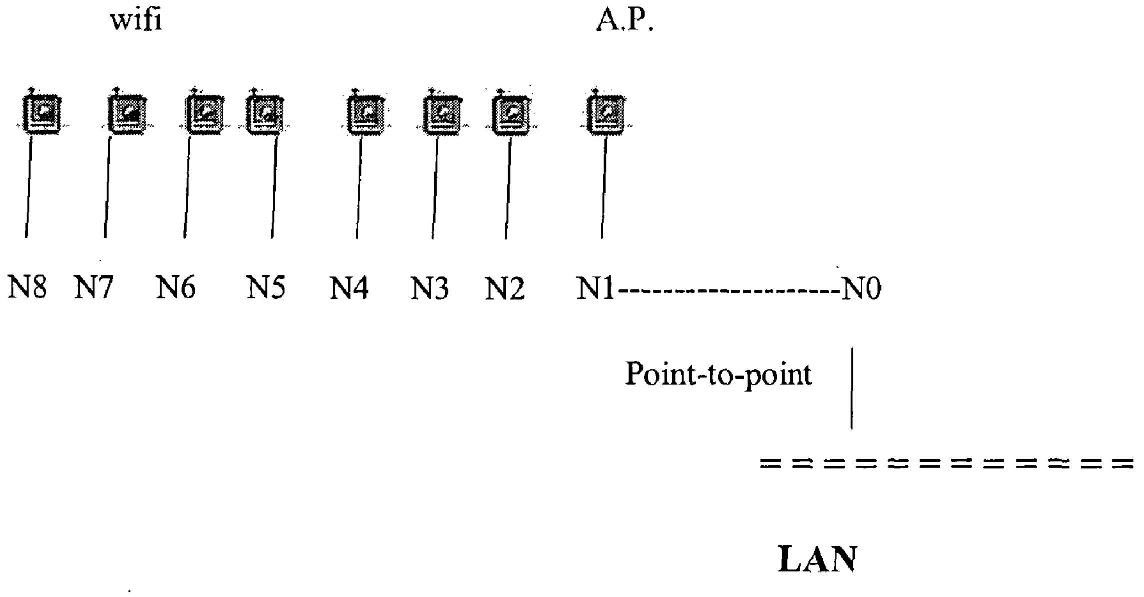

Figure 4.1: simulation topology

4.2 Simulation topology and simulation metrics

Various network scenarios were analyzed to prove the model's correctness and characteristics. Every plot was taken as an average of ten different runs. In the simulation experiment; we tested networks from 8 up to 50 mobile hosts. The nodes were placed randomly in the area of 1500m*750m to maintain the network density and connectivity as constant and balanced. In all the simulations, we used standard parameters of the channel and radio model: channel capacity of 2MB/s, free space propagation model and radio propagation range of 250 meters. The IEEE 802.11 protocol was used as the medium access control protocol.

The traffic was produced using a traffic generator, which made randomly constant bit rate (CBR) sessions. The data packet size was 512 Bytes and no fragmentation was used. The channel bit rate is 2 Mbps. The simulation time for each run is 25seconds. The results are averaged over 10 runs of the simulation.

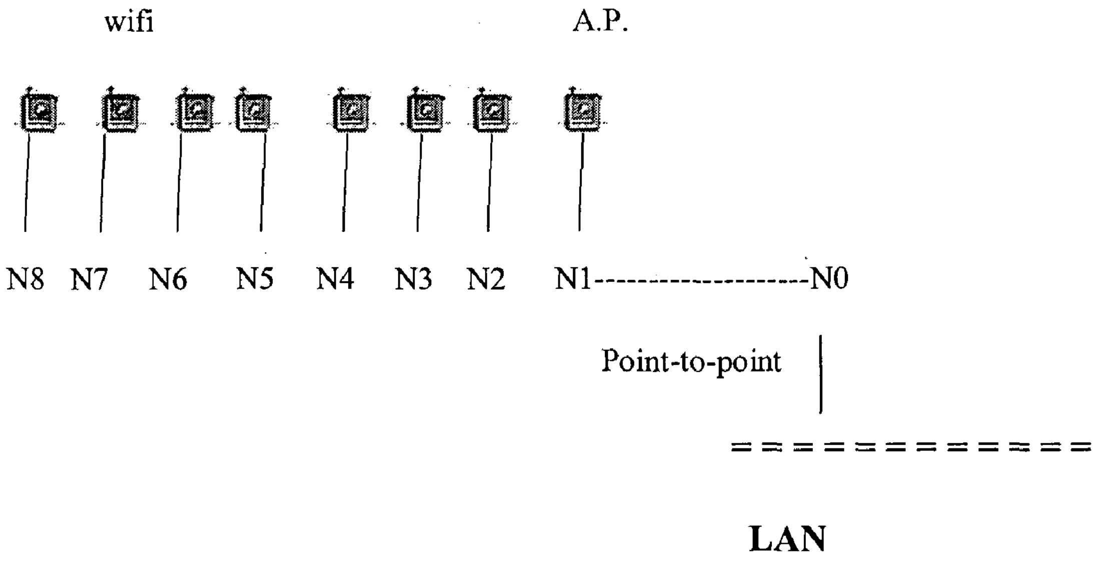

Figure 4.1: simulation topology

Simulation Metrics:

Average throughput of well-behaved hosts: This is the average throughput per well-behaved sender.

Average throughput of misbehaving hosts: This is the average throughput per misbehaving sender.

Packet Delivery Ratio (PDR) is the ratio of total no. of packets sends to total no. of packets received.

RTS retransmission at sender: it is the number of RTS frame retransmitted by sender.

parameter	**value**
Number of nodes	50
Packet size	512 bytes
Traffic model of source	Constant bit rate(CBR) of 2 Mbps
mobility	random
area	1500m * 750m
Channel bit rate	2Mbps
Simulation time	25 seconds
Number of run	10

Table 4.2: simulation parameters

4.2.1 Simulation without Selfish MAC Misbehavior

In this scenario, all nodes are using same 802.11 MAC protocol.

4.2.2 Simulation with Selfish MAC Misbehavior

In this scenario also, all nodes are using 802.11 MAC protocols except randomly chosen 5 nodes which are behaving as selfish MAC misbehaving node and communicating with each other through ALOHA as a MAC protocol . In ALOHA protocol, the node does not wait for backoff time as the MAC protocol obeying protocol does, but it transmits whenever it founds channel idle. So these two nodes, which are using ALOHA as MAC protocols will behave like the misbehaving nodes on the scenario and decrease the throughput as well as increase the packet drop ratio of all other well behave nodes by making the channel busy for other nodes. So that the number of RTS retransmission due to selfishness increases in the mesh network of other well behave nodes i.e., channel gets busy and selfish attack occurs

Chapter 5

Result and Discussion

The ideal network and the network with selfish nodes are compared on the basis of node throughput, packet delivery ratio and RTS retransmission due to time out.

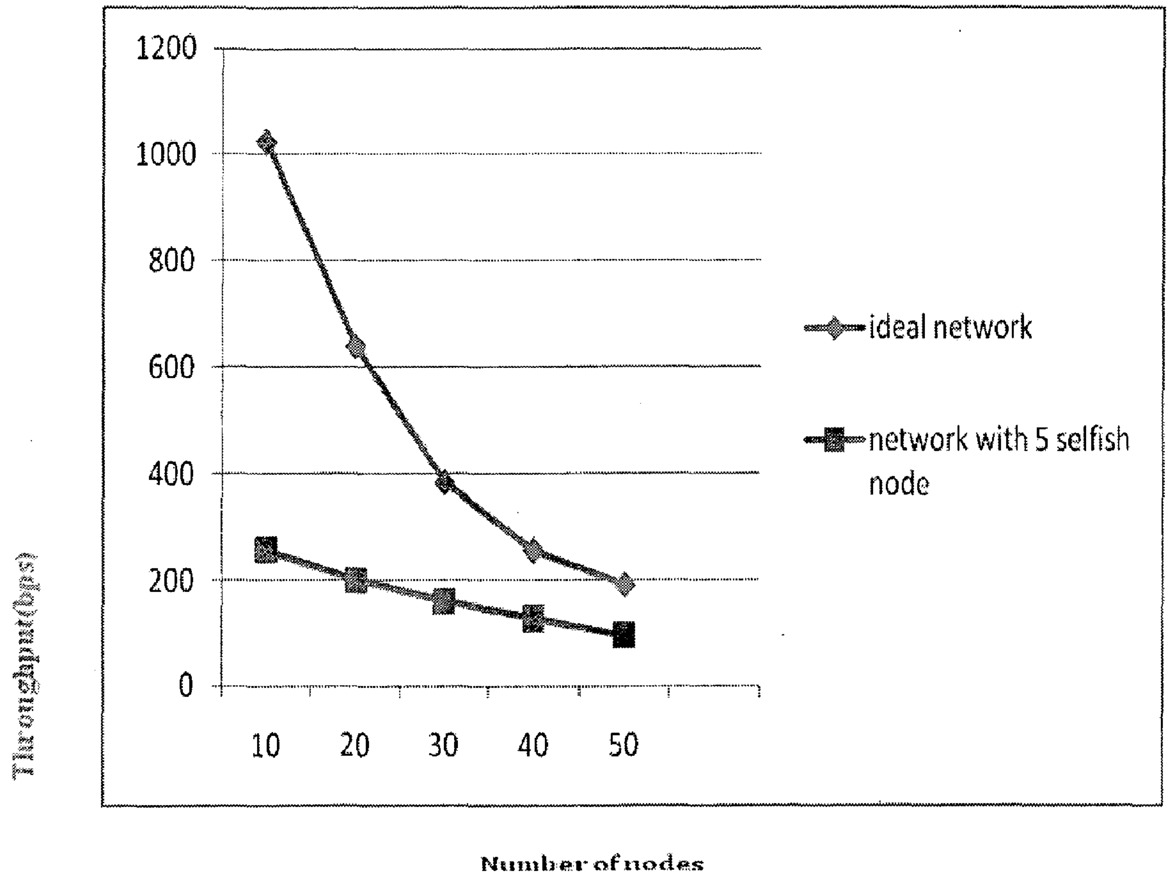

Figure5.1:Throughput comparison

Node Throughput: is the average rate of successful message delivery over a communication channel. This data may be delivered over a physical or logical link, or pass through a certain network node. The throughput is usually measured in bits per second (kbit/s or kbps). Figure 5.1 shows throughput in ideal condition and throughput when there were two selfish nodes in the network. From the figures it is shown that the throughput at node gets degraded by the presence of selfish node. The overall throughput gets degraded.

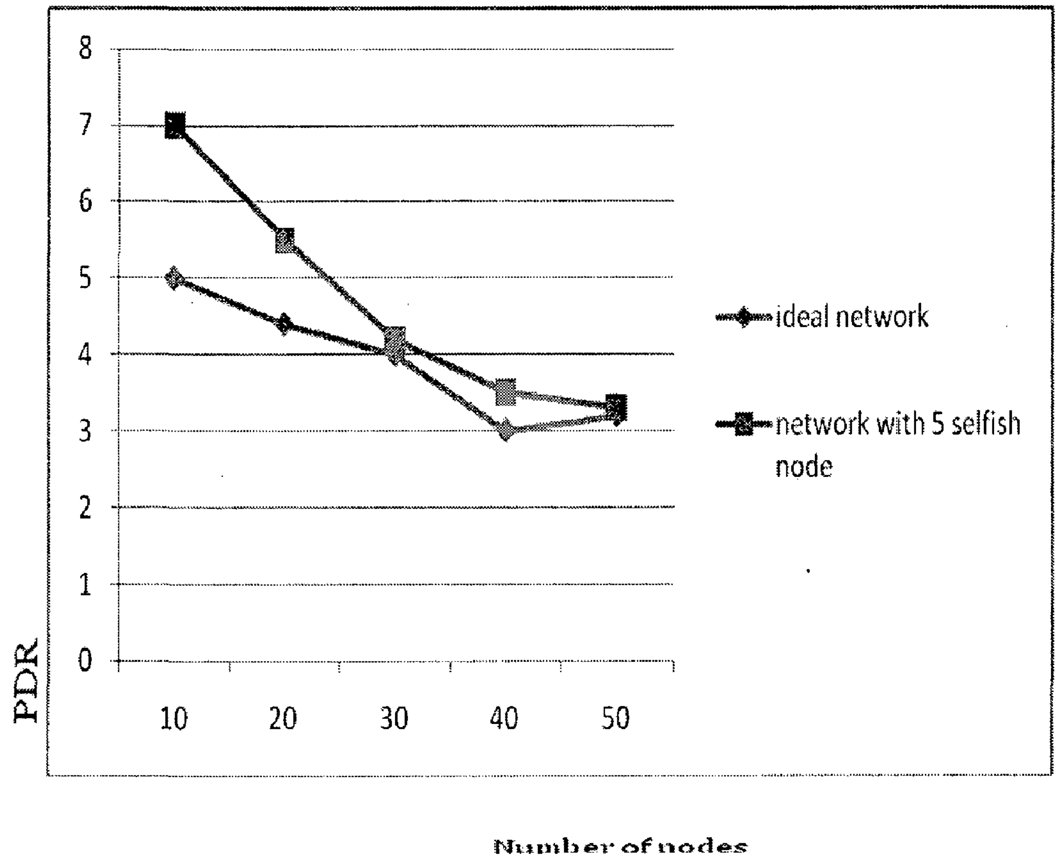

Figure 5.2: Packet retransmission rate comparison

Packet Delivery Ratio (PDR) is the ratio of total number of packets sends to total number of packets received. Figure 5.2 shows the PDR when there was no selfish node in the Network and PDR when there are selfish nodes in the network. It can be shown that the PDR increases when there are selfish nodes in the network.

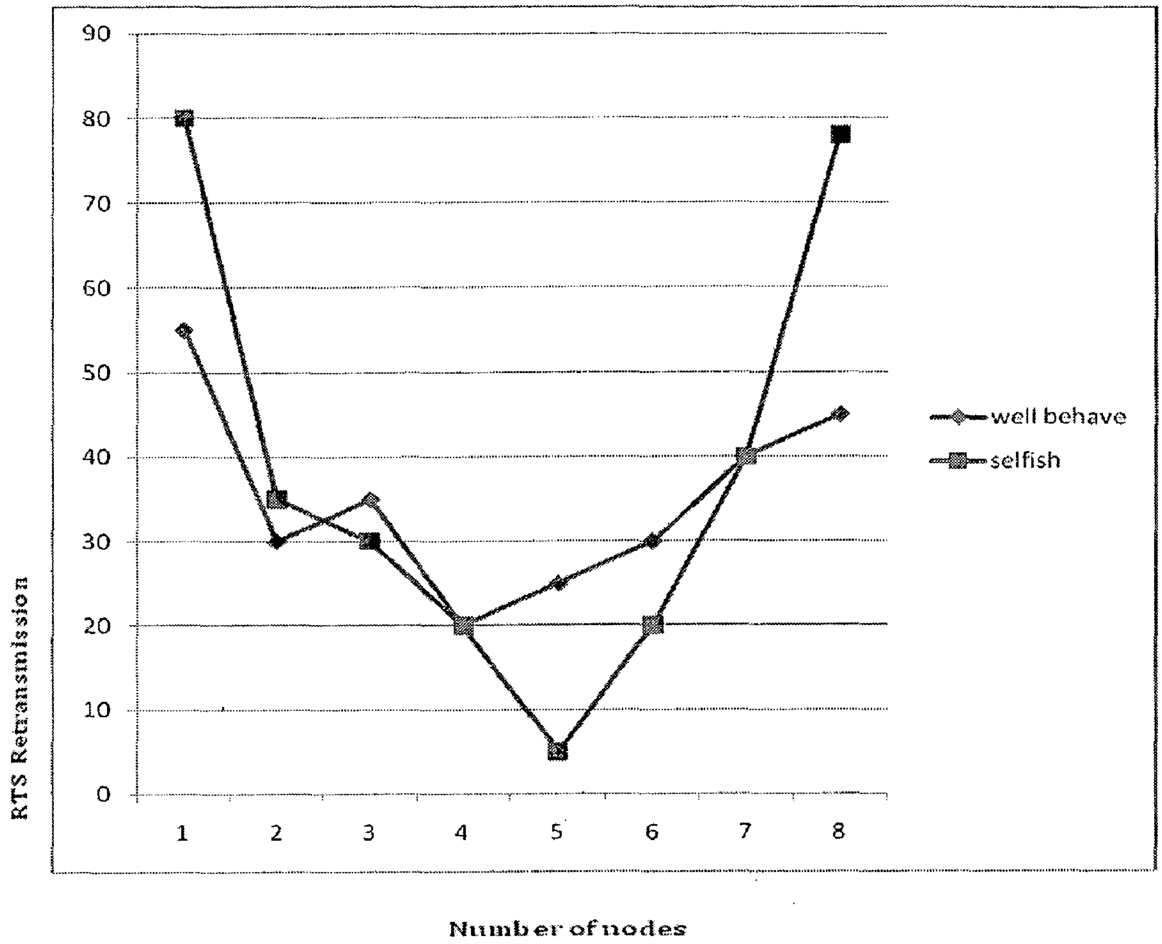

Figure 5.3: RTS retransmission rate comparison

RTS retransmission rate: We have done the simulation for 8 node with 2 selfish node.The statistical results show that the selfish node has increased the RTS retransmission rate.

In this detection scheme, first of all collect the statistical values of all nodes RTS retransmission due to time out, packet retransmission due to ACK timeout and throughput at receiver end then compare it with the threshold value. If the value is above the threshold value for RTS and packet retransmission as well as below the threshold value for throughput then selfish attack is occurring otherwise scenario is not containing any selfish nodes all are working properly without any selfishness. In Figure 5.1, 5.2 and 5.3, the statistical results show the comparative study of Throughput, RTS retransmission rate and packet retransmission rate of nodes under well behaved and selfish attack.

Chapter 6

Conclusions and Scope for Future Work

6.1 Conclusions

The statistical results show that the selfish node has increased the RTS retransmission rate and packet retransmission rate of well behaving nodes, whereas throughput degrades under selfish attack. Our proposed detection scheme for selfish MAC misbehavior in the scenario detects this attack by considering these parameters at both ends.

It has been concluded from the simulation done in NS3 that when selfish nodes are present in the network the overall network load increases on remaining nodes, hence node throughput decreases. Packet Delivery Ratio increases as nodes also forward packets which in ideal case may be forwarded by nodes which became selfish. From the above analysis, it is concluded that either misbehaving node must be isolated from the network or some system must be include with the network which enforce cooperation among nodes to improve network performance

Future work includes simulation study with malicious node and to get a system which motivate misbehaving node to enhance cooperation and improve network performance. But to pinpoint a misbehaving user is a crucial task and punishing a timid user is also necessary. We leave this for future work.

REFERENCES

[1] Y.-C. Hu and A. Perrig, "A survey of Secure Wireless AdHoc Routing," *IEEE Security and Privacy,* Special Issue on Making Wireless Work, pp. 28-39, May/June 2004.

[2] P. Kyasanur and N. Vaidya, "Selfish MAC Layer Misbehavior in Wireless Networks," *IEEE Transaction Mobile Computing*, vol. 4, no. 5, pp. 502-516, September 2005.

[3] V. Gupta, S. Krishnamurthy, and M. Faloutsous, "Denial of Service Attacks at the MAC Layer in Wireless Ad Hoc Networks," *IEEE Military Communication Conference (MILCOM)*, pp. 1118–1123, 2002.

[4] M. Raya, J. P. Hubaux, and I. Aad, "DOMINO: Detecting MAC Layer Greedy Behavior in IEEE 802.11 Hotspots," *IEEE Transaction Mobile Computing*, 2006.

[5] J. Konorski. "Multiple access in ad hoc wireless LANs with non-cooperative stations," *In NETWORKING*, volume 2345 of *LNCS*, pp. 1141-1146,Springer, 2002.

[6] R. Jain, G. Babic, B. Nagendra and C. Lam, "Fairness, Call Establishment Latency and Other Performance Metrics," Technical Report ATM Forum/96-1173, ATM Forum Document, Aug. 1996.

[7] C. He and J. C. Mitchell, "Analyzing and Improving the IEEE 802.11 MAC Protocol for Wireless LANs," *Proceedings of NDSS*, Feb. 2005.

[8] A. Cárdenas, S. Radosavac, and J. S. Baras, "Detection and Prevention of MAC Layer Misbehavior for Ad Hoc Networks," *ACM SASN*, pp.17 Oct. 2004.

[9] J. Bellardo and S. Savage, "802.11 Denial-of-Service Attacks: Real Vulnerabilities and Practical Solutions", *USENIX Symposium.*,pp.15-28, 2003.

[10] L. Guang and C. Assi, "A Self-Adaptive Detection System for MAC Misbehavior in Ad Hoc Networks," *Proceedings of IEEE ICC*, June 2006.

[11] L. Guang, C. Assi, and A. Benslimane, "Modeling and Analysis of Predictable Random Backoff in Selfish Environments," *Proc. ACM/IEEE MSWiM*, pp.86,Oct. 2006.

[12] S. Djahel and F. Na Abdesselam, " FLSAC: A New Scheme to Defend Against Greedy Behavior in Wireless Mesh Networks", *International Journal of Communication Systems (IJCS)*, Wiley InterScience Publisher, 22(10):1245-1266, jun. 2009.

[13] IEEE Standards for Wireless LAN-Medium Access control and Physical Layer Specification, P802.11, 1999.

[14] NS3 home page. [Online Availale] http://www.nsnam.org/

[15] P. Pavon and S. Choi, "Link adaptation strategy for ieee 802.11 wlan via received signal strength measurement," in *IEEE International Conference*,vol. 2, 11-15 May 2003, pp. 1108–1113.

[16] S. Savage, N. Cardwell, D. Wetherall, and T. Anderson, "TCP Congestion Control with a Misbehaving Receiver,"*ACM Computer Communications Review*, pp.71-78, October 1999.

[17] D. Ely, N. Spring, D. Wetherall, S. Savage, and T. Anderson, "Robust Congestion Signaling," in *Proceedings of the 2001 International Conference on Network Protocols*, pp.332,Riverside, CA, November 2001.

[18] A. B. MacKenzie and S. B. Wicker, "Stability of Multipacket Slotted Aloha with Selfish Users and Perfect Information," in *Proceedings of Infocom 2003*, vol. 3, pp.1583 ,San Francisco, CA, IEEE, April 2003.

[19] J. Konorski, "Multiple Access in Ad-Hoc Wireless LANs with Noncooperative Stations,"*proc. in NETWORKING*, volume 2345 of LNCS, pp.1141, Springer, 2002.

[20] D. J. Burroughs, L. F. Wilson, and G. V. Cybenko, "Analysis of Distributed Intrusion Detection Systems Using Bayesian Methods," in *Proceedings of IEEE International Performance Computing and Communication Conference*,pp.329-334,April 2002.

[21] Matthias Hollick, jens Schmitt, Christian seipl, "On the Effect of Node Misbehaviour in Ad hoc Network," *IEEE conference* , vol 6, pp 3759-3763,2004.

[22] S. Capkun, J.-P. Hubaux, and L. Buttyan, "Mobility helps security in ad hoc networks," *Proceedings of the 4th ACM Symposium on Mobile Ad Hoc Networking and Computing*, pp. 46–56, Annapolis, Maryland, USA, 2003

[23] M. Conti, E. Gregori, and G. Maselli, “Cooperation issues in mobile ad hoc networks,” in *24th International Conference on Distributed Computing Systems Workshops W6:WWAN (ICDCSW’04)*, pp. 803–808, Mar 23-24, 2004, Hachioji, Tokyo,Japan.

[24] S. Seth and A. Gankotiya. “Denial of service attacks and detection methods in wireless mesh networks”. In *Recent Trends in Information, Telecommunication and Computing (ITC), International Conference on*, pages 238 –240,march 2010.

[25] M. Arora, R.K. Challa, and D. Bansal. “Performance evaluation of routing protocols based on wormhole attack in wireless mesh networks”. In *Computer and Network Technology (ICCNT)*, 2010 *Second International Conference* on,pages 102–104,april 2010.

[26] D.M. Shila and T. Anjali. “Defending selective forwarding attacks in wmns”. In *IEEE International Conference on Information Technology*, pages 96 –101, may 2008.

LIST OF PUBLICATIONS

[1] Vivek Muskan, "Detection of misbehavior at MAC layer in wireless network," *International Conference on Computer Science and Informatics (ICCSI-2011)",* Bangalore, India, 24-25 July, 2011 (Accepted).