CHAPTER 2

BACKGROUND AND RELATED WORK

2.1 BACKGROUND OF IEEE 802.11 MAC PROTOCOL

Wireless networks have experienced unparalleled development in the past decade. IEEE 802.11 MAC uses two types of coordination function to access the wireless networks. Firstly, Distributed Coordination Function (DCF), which allows contention access for wireless channel and secondly, Point Coordination Function (PCF), which requires centralized APs. The architecture of the IEEE 802.11 MAC is shown in Figure 2.1.

The contention resolution mechanism is typically based on cooperative protocols (e.g., random backoff before transmission) that attempt to ensure a reasonably fair throughput share for all the participating hosts. In environments where hosts in the network are untrusted, some hosts may misbehave by failing to adhere to the network protocols, with the intent to obtain an unfair share of the channel. PCF is the upper sublayer and DCF is the lower sublayer in the MAC protocol. PCF is a contention free access protocol, which is controlled by centralized point coordinator to support real time traffic. The main drawback of PCF is that it will not work for MANET due to the central coordinator and also it is not commonly supported in commercial products.
DCF is a random access method, which uses Carrier Sensing Multiple Access with Collision Avoidance (CSMA/CA) to access and reduce the packet collisions. In CSMA/CA networks, a radio station which finds that the radio environment is available will start to transmit only after random backoff procedure (Potorac 2009). Any node which wishes to transmit will first sense the channel to know the status of the medium (busy/idle). If the medium is busy, the node defers its transmission until the medium is determined to be idle for a duration which is equal to DIFS. If the node is idle for DIFS time, it then enters into the backoff window or contention window. Backoff time is a random value which can be chosen uniformly from the range 0 to \( CW_{\text{min}} - 1 \), where \( CW_{\text{min}} \) is the minimum contention window size with a standard value of 32 and the maximum contention window size is set to 1024. When the channel is sensed idle, the backoff timer is decremented for every time slot and freezes when the medium is sensed busy. When the
backoff timer reaches 0, the node starts its next transmission. The node doubles the contention window for each unsuccessful transmission until it reaches the maximum value \( CW_{\text{max}} = 2^m CW_{\text{min}} \), where \( m \) is the maximum backoff stage with a standard value of 5. This is known as Binary Exponential Backoff (BEB) algorithm. This will reset to minimum contention window after each successful transmissions (Tang et al 2012). The backoff value is expressed by the following equation:

\[
\text{Backoff Counter} = \text{INT} (\text{Rnd}().CW_{\text{min}})
\]

where, \( \text{Rnd}() \) is a function that returns pseudorandom numbers uniformly distributed in \((0, 1)\) (Cagali et al 2004).

DCF defines two types of carrier sensing mechanism. First one is called physical carrier sense, which is supported by the physical layer. Second one is virtual carrier sense, which is supported by the MAC layer.

2.1.1 Basic Access Method

DCF includes both basic access method and an optional channel access method using Request To Send / Clear To Send (RTS/CTS) exchanges. Basic access mechanism is a two way handshaking method where only data and ACK are exchanged which is shown in Figure 2.2. When the transmitter transmits data to the receiver after Short Inter-Frame Space (SIFS) interval, the receiver replies with the ACK control frame. If ACK is not received by the sender within the specified ACK_Timeout period then, the frame is assumed to be lost and schedules the retransmission.
2.1.2 RTS-CTS Mechanism

In RTS/CTS access method, when the node needs to transmit a data frame it should wait until the channel is sensed idle for DIFS time and backoff time. Then only the node can transmit short RTS control frame instead of data frame. After a SIFS interval the receiver replies with the short CTS control frame. This RTS/CTS exchange ensures that both the sender and receiver are ready to transmit and receive the frames which are shown in Figure 2.3.
Figure 2.3 IEEE 802.11 RTS/CTS mechanism

Both the RTS and CTS frames contain details about the length of the frame to be transmitted. Neighbouring nodes which overhear the RTS and CTS control packets will update their Network Allocation Vector (NAV). NAV is a timer which is included in the duration field of RTS, CTS control frames. When the NAV timer becomes 0, neighbouring nodes can start their transmission, otherwise it would be silent. Now the sender sends data packets after the SIFS interval. The receiver replies with ACK to confirm the reception of the data packets. SIFS period is shorter than the DIFS period, which guarantees continuous RTS+CTS+DATA+ACK exchange (Konorski 2006).

2.1.3 Misbehaving Techniques

In the Data link layer, in order to achieve an operational point in the network, all the CSMA/CA schemes assume that all participants should strictly follow the protocol specifications. However, especially in the presence of autonomous nodes this assumption may not always be valid. Unfortunately,
there are various ways in which a station can gain advantage by not adhering to the protocol guidelines like:

- Choosing small backoff values: A selfish node can choose a smaller value instead of choosing randomly.

- Not doubling CW after collision: A node may not invoke the collision recovery procedure after collision. Thus, the node would always be choosing its backoff values from \([0, \text{CW}_{\text{min}}]\), thereby utilizing values for backoff.

- Manipulating the NAV value: If a node increases this value, it can assure that all other agents will remain idle even after the end of current transmission.

- Not confirming to the DIFS and SIFS intervals: This behavior will increase the chances of getting access to the medium.

- Magnify the value of the duration field in RTS or DATA packets such that the receivers keep silence for a period larger than the real transmission time. As a result, if the cheater node has more packets to send, it gets more chance to access the medium, as it starts counting down its backoff before its neighbors.

- When the channel is sensed to be idle, it transmits before the required DIFS time slots elapses, i.e. the misbehaving node waits for a shorter period called S-DIFS (Short-DIFS).
2.2 LITERATURE REVIEW

2.2.1 Introduction

Although IEEE 802.11 has become more and more popular due to its low cost and easy deployment, it does not provide security support. Most of the research work, which deals with wireless security is primarily focused on addressing malicious misbehavior, which disrupts normal network operation with no performance gain to the misbehaving node. In contrast, researches addressing selfish misbehavior, assume that selfish hosts misbehave primarily to improve their own performance such as throughput, latency, energy etc.

Selfish misbehavior includes hosts that refuse to forward packets on behalf of other hosts to conserve energy. Nodes select small backoff values to obtain large throughput share than the well behaved nodes. Malicious misbehavior includes DoS attacks that disrupt routing operation, TO attack (the misbehavior that we addressed here), jamming the wireless channel to prevent communication, etc (Hubaux et al 2001).

Several approaches have been proposed for addressing malicious misbehavior at the data link layer, but each approach has some advantages and drawbacks. Security improvement in MANET is based on the detection and prevention of malicious nodes participating in the network and also by reducing the collision between nodes. Based on these, the literature review has been carried out.

2.3 REVIEW BASED ON MAC LAYER MISBEHAVIOR

Kyasanur & Vaidya (2005) have proposed the MAC layer misbehavior through the modification of the IEEE 802.11 MAC protocol, in order to detect and penalize the selfish misbehavior. Here the receiver assigns
back off value to the sender using RTS and ACK control packets. The sender uses this assigned back off value in the next transmission.

Lolla et al (2006) have modified the IEEE 802.11 MAC protocol and has proposed the method to detect the MAC layer backoff timer violations in MANETs. In this method, the random number generator state exchanges the random number generated to every neighbour. After that wilcoxon rank sum test is used to detect the misbehavior. This test uses the fixed sample size to compare the difference between analytically computed samples and the observed sample size. The disadvantage of this approach is the use of the fixed sample size to detect the misbehaving node and also it does not handle collusion between nodes.

2.3.1 DOMINO – Access Point Trusted

Raya et al (2006) has proposed a detection system called DOMINO. It does not require any modifications in the IEEE 802.11 MAC protocol. The DOMINO is implemented at the AP and it is assumed to be trusted. The sender nodes traffic is collected periodically during short intervals of time called monitoring period. This collected data is passed to the DOMINO algorithm for several tests which is used to detect the backoff manipulation and oversized NAV. The result of each test is fed into the check procedure, which indicates that whether a particular station is misbehaving or not. The node misbehavior can be found using the corresponding cheat counter threshold.

2.3.2 Dream System

Dream system (Guang et al 2007) is used to detect the TO attack either at the transmitter side or receiver side. It does not require any modification in the IEEE 802.11. There are two procedures, namely detection
and reaction, which is used to detect the misbehaving node. The first reaction stage is used to mitigate and the second reaction stage is used to punish the misbehaving node. After the node suspects a misbehaving, then the second reaction procedure is called. It needs to generate the long term monitoring process to evaluate the trust level, where each node maintains a trust level list. However, it requires two reaction procedures, besides the minor changes in the existing standard to reduce the number of protocol failure or the misuse.

2.3.3 Game-Theoretic Approach

A game model was proposed by Cagali et al (2004) to detect the MAC layer misbehavior. Each node follows the channel assess probability by controlling the adjustment of contention window using the dynamic game model. Here, the network receives its equilibrium assuming that all the nodes are within the transmission range, in order to avoid the hidden terminal problem. Hence, this scheme may not be suitable for ad hoc environments, instead it works well in wireless LAN environment.

Yang et al (2005) has proposed an adaptive backoff window congestion control algorithm to maximize the total utilities with heterogeneous users, where either selfish users or non cooperative environment is not being considered. Borkar & Kherani (2004) suggested a non cooperative game using random access protocol. This method doesn’t have the difference between benefit of successful transmission and inconvenience caused by the collision. The disadvantage of this method is that it maximizes each user’s selfish objective. IEEE 802.11 MAC protocols modifications are not considered.
2.3.4 Minimax Robust Misbehavior Detection

Minimax robust misbehavior detection (Radosavac et al. 2005) constitutes the theoretical worst case attack framework to detect the misbehaving nodes. Here, all the transmissions are observable during communication. But, in the case of a collision, it is not possible to obtain which node get involved in the communication. There is no operational method proposed to detect the misbehaving node. Deng et al. (2008) suggested that a Carrier Sensing based Discarding scheme (CSD) was used to detect the misbehaving node. This method needs several carrier sensing points which are randomly deployed for the entire packet transmission period.

2.3.5 Kolmogorov-Smirnov (K-S) Test

Toledo & Wang (2007a) utilizes the Kolmogorov-Smirnov (K-S) test to address the detection problem. The misbehavior detection can be made by comparing the distribution of sampled traffic data with the normal behavior distribution estimated on line. This method needs fixed size data samples to perform the operation which are not suitable for real time detection. In the modified sequential truncated K-S test (Toledo & Wang 2007b), the number of samples N should be predefined before the test starts, in order to get a proper significant level for each test step.

In order to ensure the randomness of the backoff value, a new approach is proposed by Cardenas et al (2004), in which at least one of the communicating nodes (sender or receiver) is assumed to be honest and a reputation system such as CONFIDANT is deployed at MAC layer. The idea of this work is to let both the sender and receiver agree on a random value of backoff through a public discussion.
2.3.6 Cryptography Concept

A small cryptography concept is used to produce an improvement ensuring randomness of each backoff time i.e., the sender cannot be punished without a reason, while being unable to launch an undetected backoff attack (Cardenas et al 2004). The RTS+CTS+DATA+ACK exchange is a vehicle for a coin flipping scheme. The recipient commits to a random value R by announcing its hash ˜R in the CTS frame. Similarly the sender appends another random value S to the DATA frame and finally the recipient announces R in the ACK frame, whereupon the next backoff time is computed with the bit-by-bit exclusive-OR of R and S. The misbehaving nature is detected when the hash of R does not match ˜R and can be reported to the sender.

2.3.7 Sequential Probability Ratio Test (SPRT)

Rong et al (2006) introduced a more technical approach, where the detection algorithm relies on the sequential probability ratio test. The observations of the detection agent are not the back-off times of the stations, instead it is the inter-delivery time distribution. To use the SPRT test, they estimate a normal inter-delivery distribution and an attack inter-delivery distribution. Within the min-max robust detection framework, the robust SPRT addresses the detection of an adaptive intelligent attacker by casting the problem of misbehavior detection (Radosavac et al 2008).

2.4 REVIEW BASED ON OPTIMIZATION TECHNIQUE

Baker & Ephremides (2003) proposed identifier-based clustering algorithm known as lowest-ID. It assigns a unique ID to each node and whenever a new node with a lowest ID appears, the cluster-head is replaced. Gerla & Tsai (1995) proposed the highest connectivity clustering algorithm. It
is a wireless adaptive mobile information systems with multi-cluster, multi-hop packet radio network architecture. In this technique the degree of nodes is calculated, which is the number of neighbours of a given node. During the election procedure, each node broadcasts its identifier. After computing its degree, the node having the maximum degree becomes the cluster-head.

A genetic algorithm based on clustering algorithm, proposed by Das et al (2002) was used to optimize the number of clusters in an ad hoc network. It is a weight-based clustering algorithm which assigns a weight set by the user to each objective of the problem. Chatterjee et al (2002) proposed the weighted clustering algorithm which elects cluster heads according to their weights. All the weights are computed by combining the set of parameters such as battery power, mobility and transmission range and is the first weighted clustering algorithm proposed for MANETs.

Constrained optimization is one of the game-theoretic contexts used (Fang & Bensaou 2004), concentrated on the rarely addressed issue of selfish MAC-layer behaviour in multihop IEEE 802.11 MANETs. In a conceptual link contention graph, the vertices are station-to-station wireless links which means the two stations are within each other’s transmission range. The vertex adjacency reflects the sender or recipient of one link which is within the interference range of the sender or recipient of the other.

In another implementation, the feedback from the network is used for CW adjustments, with increased collision rates and queuing delays indicating that a clique capacity is being approached. This solution may appear like it is not “purely” game-theoretic, since clique capacity constraints are exogenous. The common issue is that, a station sending a flow down the next link along an end-to-end path should be concerned about flows on other links. However, some other links of a clique may be used by the flow further down the path and so reflect upon the flow’s satisfaction. The solution does
not require station authentication and it is not applicable to ad hoc LANs. Here, the maximal clique covers the entire network and no capacity constraint keeps the nash equilibrium away from “all-greedy” i.e., it finally concludes that there is a uniform incentive to launch a backoff attack.

2.5 REVIEW BASED ON COLLISION

Based on the RTS/CTS scheme, many MAC protocols are proposed to avoid data collision (Garcés & Garcia 1996). The success of the RTS transmission depends mostly on the performance of these protocols. Some research’s make use of the concept of additional channel(s) to alarm itself for transmission, in order to preclude others interference (Ye et al 2004). However, seldom in the literature it was proposed to prevent from the RTS collisions. Park & Sivakumar (2002) considered traffic load which evaluated the collision effect on network performance. All of the above protocols pointed out that contention-based MAC protocols are easy to encounter RTS collisions, especially in heavy traffic load and subsequently, degrades the network throughput and performance. Moreover, the behaviour of RTS/CTS handshaking analysis results in the probability of RTS collisions in any contention-based scheme to be higher than existing.

2.5.1 Jamming Based MAC Protocol

Similar to the tone concept of DBTMA (Haas & Deng 2002), Ye et al (2004) have proposed a jamming-based MAC protocol, namely JMAC, which divides the shared medium into two sub channels, S channel and R channel. The RTS and data frames are transmitted on the S channel whereas the CTS and ACK frames on the R channel. As a result, each STA should also be attached with two transceivers to monitor the S and R channels status respectively. DBTMA and JMAC are based on the same concept of the busy tone or the jamming signal where the receiver can protect its receiving.
However, the two schemes still fail in avoiding the RTS collisions caused by the hidden terminals.

### 2.5.2 Floor Acquisition Multiple Access with Non-Persistent Carrier Sensing

The Floor Acquisition Multiple Access with Non-Persistent Carrier Sensing (FAMANCS) scheme (Fullmer & Garcia-Luna-Aceves 1997) uses long dominating CTS packets, in order to act as a receiver busy tone to prevent any competing transmitters in the receiver’s range from transmitting. This indirectly instructs each node hearing the interference to keep quiet for a period of one maximum data packet, to guarantee no collision with the ongoing data transmission. This is not efficient especially when the RTS/CTS negotiation process fails or the data packet is very short. Multi-channel random MAC schemes have also been investigated here (You et al 2003).

One common approach to avoid collisions is to use separate channels for different kinds of packets between control packets and data packets. The On Demand Channel Assignment (DCA) scheme (Wu et al 2000a) uses one control channel for RTS/CTS and one or more data channels for DATA/ACK. However, it does not overcome the hidden terminal problem. The dual busy tone multiple access used in DBTMA schemes (Wu et al 2000b) uses a transmit busy tone to prevent the exposed terminals from becoming new receiver. Also the receiver prevents the hidden terminals from becoming new transmitter and a separate data channel is also used to avoid collisions between control packets and data packets. However, the DBTMA schemes have no acknowledgements for data packets, which are needed for unreliable wireless links. Also the potential collisions between the acknowledgements and other packets can greatly degrade the performance.
A scheme that uses a fixed value of large RCS has been proposed to improve fairness of wireless ad hoc networks and to reduce interferences (Zhou 2005). Although it can avoid all interferences, probability of exposed terminal problem was significantly increased. Some of the researchers used tunable Physical Carrier Sensing (PCS) under some network conditions (Zhu et al 2004). Several current 802.11 WLAN chips also support one or more parameters to control PCS for adaptively tuning RCS.

2.5.3 Receiver-Initiated Busy-Tone Multiple Access Protocol

A receiver-initiated busy-tone multiple access protocol for packet-radio networks has been proposed to eliminate the hidden node problem (Wu & Li 1987). In this scheme, prior to sending the data packet, a sender transmits an RTS to the receiver. After receiving the RTS by the receiver, it separately transmits a busy-tone to alert other channel solution to this node nearby to back-off their transmissions. The corresponding source node is notified that it can proceed with the transmission of data packet. The main drawback of this scheme is the use of an additional separate channel for busy-tone messages transmission.

RTS/CTS exchange (later adopted by IEEE 802.11 design group) can be more effective when all of the hidden nodes are in transmission range of the receiver. But this assumption does not always hold to be perfect because there will be many nodes outside the transmission range of the sender-receiver and collisions may occur. In multi-hop ad hoc networks, hidden nodes will often create a serious problem, since the nodes are scattered in the transmission area and the above-mentioned collision problem can frequently occur (Kanth et al 2002).
Gupta & Kumar (2000) has proposed that regardless of the problems exist in the MAC sub-layer, the per-node throughput declines as the number of nodes grows in the network. He has assumed a saturated network in which the nodes always have data to send and are ready to transmit as fast as their wireless connections allow.

Chung & Liew (2004) tried to eliminate the performance problems in wireless networks through “offered load control” at data sources without imposing major changes on MAC protocol. They argue that controlling the data rate in sources can mitigate some of the problems that may emerge along the path.

Acharya et al (2003) has proposed the initial design of MACA-P, which mainly targeted for allowing simultaneous transmissions in multi-hop ad hoc networks. It avoids collisions and improves the system throughput by delaying the data transmissions by a control phase interval which allows multiple sender-receiver pairs to synchronize their data transfers.

### 2.6 PERFORMANCE METRICS

Before carrying out experimental evaluation of the proposed protocol through simulation, it is intrusive to identify the basic parameters on which an evaluation should be based. The various performance parameters like throughput, packet delivery ratio, delay, jitter, misdetection and correct detection ratio, number of RTS-CTS collisions are discussed here. The definitions of the above considered parameter are as follows.
2.6.1 Throughput

It is defined as the amount of data moved successfully from the sender to receiver in a given time period. Data transfer rate for networks are measured in terms of throughput. Typically throughputs are measured in Kbps, Mbps, Gbps.

2.6.2 Packet Delivery Ratio

It is defined as the ratio of data packets received by the destinations to those generated by the source.

Mathematically, it can be defined as $PDR = \frac{s1}{s2}$

where, $s1$ is the sum of data packets received by each destination and $s2$ is the sum of data packets generated by each source.

2.6.3 End to End Delay

It is defined as the average time of a data packet to reach the destination. It includes all possible delays caused by buffering during route discovery latency and queuing at the interface queue. The end-to-end delay is represented in milliseconds (ms).

2.6.4 Jitter

The delay is specified from the start of the packet being transmitted at the source to the end of the packet being received at the destination. A component of the delay which does not vary from packet to packet can be ignored. Hence if the packet sizes are the same then the packets always take
the same time to be processed at the destination. The packet arrival time at the destination is used instead of the end time the packet is received.

i.e., it is the difference of the latency of the current and previous packet. The jitter is represented in milliseconds (ms).

2.6.5 Correct Detection Ratio

It is the ratio of number of misbehaved nodes that are correctly marked by the detection system as suspects to the total number of active misbehaved nodes in the network.

2.6.6 Misdetection Ratio

It is the ratio of the number of well-behaved nodes that are incorrectly diagnosed as suspects to the total number of well-behaved nodes in the network.

2.7 DISCUSSION

The major research activities on MANETs are towards the detection and prevention of MAC layer misbehavior. The objective of the mobile ad hoc research is to improve the security, by minimizing the number of malicious nodes participating in the network.

This chapter mainly concentrates on the frequently addressed issue of malicious MAC layer which is proposed in the literature for multihop IEEE 802.11 MANETs. These have been categorized based on the modifications of MAC protocol, without changing the MAC protocol. These methods have their own pros and cons. Based on the modification scheme, it creates
computational overhead due to the addition of new frame header in the control packets.

For ad hoc networks, dynamic game model is not suitable when compared to wireless LAN environment. In certain cases, there are no operational methods proposed to detect the misbehaving node while in others, the receiver is assumed to be trusted. Many MAC protocols are proposed to avoid the collision during the transmission. Some methods make use of the concept of additional channels to alarm in order to prevent the interference. It avoids the collision even in the heavy network traffic but the implementation of the hardware cost is high. Based on the analysis, there is still scope for detecting the malicious nodes and preventing the collision to improve the security. The performance parameters of the MAC protocol, which is used to evaluate the proposed methods have been discussed in this chapter.

### 2.8 DEVELOPMENT TOOLS

#### 2.8.1 Network Simulator-2 (NS-2)

NS-2 is a one of the simulation tool designed especially for communication networks. The main functionalities of NS-2 are to set up a network of connecting nodes and to pass packets from one node to another.

NS-2 is an open-source event-driven simulator designed specifically for research in computer networks for communication. NS-2 was launched in 1989, has continuously gained tremendous interest from academia, industry and government. It was under constant investigation and enhancement for many years and now NS-2 contains modules for numerous network components such as transport layer protocol, routing, application etc.
Undoubtedly, among the simulation tools available, NS-2 has become the most widely used open source network simulator used by various people and in research field.

A network object is one of the main NS-2 components which is responsible for packet forwarding. The polymorphism concept in Object-Oriented Programming (OOP) is used to implement network objects in NS-2.

Figure 2.4 shows the basic architecture of NS-2. This provides an executable command ‘ns’ which takes an input argument and which is the name of a Tcl simulation scripting file. In most cases, a simulation trace file is created and is used to plot graph or to create animation.

NS-2 consists of two key languages: C++ and Object-oriented Tool Command Language (OTcl). The C++ coding defines the internal mechanism (i.e., a backend) of the simulation objects, which is the hidden part, whereas the OTcl sets up simulation by assembling and configuring the objects as well as scheduling discrete events (i.e., a frontend). The C++ and the OTcl coding are linked together using TclCL. The variables in the OTcl domains are
mapped to a C++ object and are sometimes referred to as handles. Conceptually, a handle (e.g., n as a Node handle) does not contain any functionality and is just a string (e.g., _o10) in the OTcl domain. Instead, the functionality is defined in the mapped C++ object. In the OTcl domain, to interact with users and other OTcl objects, the handle will act as a frontend. It may define its own procedures and variables to facilitate the interaction. It is noted that the member procedures in the OTcl domain are called instance procedures (instprocs) and variables are called instance variables (instvars), respectively (Schildt 2002).

Large numbers of built-in C++ objects are available in NS-2. It is mandatory to use these C++ objects using a Tcl simulation script to set up a simulation. However, advance users may find these objects are still insufficient. They need to develop their own C++ objects for the already built-in objects and use a OTcl configuration interface to put together these objects with the help of a handle. After simulation, the NS-2 outputs which are both text-based or animation-based simulation results such as NAM (Network AniMator) and XGraph are used. To analyze a particular behavior of the network, users can extract a relevant subset of text-based data and transform it to a more conceivable presentation.

The details of discrete-event simulation in NS-2 are described in this chapter. The simulation is initially carried out by running a Tcl simulation script, which consists of two parts. Firstly, the Network Configuration Phase establishes a model network, and configures/initiates all simulation components. This phase is also responsible for creating a chain of events by connecting the created events chronologically. Secondly, the Simulation Phase executes the created events until the simulator is stopped, or until all the events are executed.