Bachelor of Science in Computer Science and Engineering

Improving Detection, Prevention and Reaction of Selective Jamming Attack Using Packet Hiding Method

Moinoddeen Quader Al Arabi
ID: 1204120

November, 2017

Department of Computer Science & Engineering
Chittagong University of Engineering & Technology
Chittagong-4349, Bangladesh.

Improving Detection, Prevention and Reaction of Selective Jamming Attack Using Packet Hiding Method

This thesis is submitted in partial fulfillment of the requirement for the degree of Bachelor of Science in Computer Science & Engineering.

Moinoddeen Quader Al Arabi
1204120

Supervised by
Mohammad Obaidur Rahman
Assistant Professor
Department of Computer Science & Engineering (CSE)
Chittagong University of Engineering & Technology (CUET)

Department of Computer Science & Engineering

Chittagong University of Engineering & Technology

Chittagong-4349, Bangladesh.

November, 2017

The thesis titled **“Improving Detection, Prevention and Reaction of Selective Jamming Attack Using Packet Hiding Method”** submitted by ID No. 1204120, Session 2015-2016 has been accepted as satisfactory in fulfillment of the requirement for the degree of Bachelor of Science in Computer Science & Engineering (CSE) as B.Sc. Engineering to be awarded by the Chittagong University of Engineering & Technology (CUET).

Board of Examiners

1.____ Chairman
(Supervisor)
Mohammad Obaidur Rahman
Assistant Professor
Department of Computer Science & Engineering (CSE)
Chittagong University of Engineering & Technology (CUET)

2.____ Member
Professor Dr. Mohammad Shamsul Arefin (Ex-officio)
Head of the Department
Department of Computer Science & Engineering (CSE)
Chittagong University of Engineering & Technology (CUET)

3.____ Member
Abu Hasnat Mohammad Ashfak Habib (External)
Assistant Professor Department of CSE
Department of Computer Science & Engineering (CSE)
Chittagong University of Engineering & Technology (CUET)

Statement of Originality

It is hereby declared that the contents of this project are original and any part of it has not been submitted elsewhere for the award if any degree or diploma.

------------------------------------ ------------------------------------

Signature of the Supervisor **Signature of the Candidate**

Date:

Acknowledgment

First and foremost, I would like to thank Allah for the good health and well-being that were necessary to complete this work. I wish to express my sincere gratitude to my honorable project Supervisor **Mohammad Obaidur Rahman**, Computer Science and Engineering, Chittagong University of Engineering and Technology for providing me the perfect guidance, encouragement, instructive suggestions with all the necessary facilities for the research and preparation for the project. I place on record, my sincere thank you to **Dr. Mohammad Shamsul Arefin**, Head of the Department, Department of Computer Science and Engineering, Chittagong University of Engineering and Technology for the kind encouragement. I also grateful to our external, **Abu Hasnat Mohammad Ashfak Habib**, Assistant Professor, Department of Computer Science and Engineering, Chittagong University of Engineering and Technology, for his guidance and review of our project work. I take this opportunity to express gratitude to all of the Department faculty members and seniors for their help and support. I also thank my parents for the unceasing encouragement, support, and attention. I also place on record, my sense of gratitude to one and all, who directly or indirectly, have lent their hand in this venture.

Abstract

Sensors consist of various constraints, which make the network challenging for communicating with its peers. Jamming is a serious threat in wireless sensor networks. Jamming attacks can severely affect the performance of Wireless Sensor Networks (WSNs) due to their broadcast nature. The open nature of the wireless medium creates the chances of intentional interference attacks, typically referred to as jamming. And this jamming leads to Wireless Denial of Service (DoS). Anyone with a transceiver can eavesdrop on wireless transmissions, inject spurious messages, or jam legitimate ones. The adversary interferes with the reception of messages by transmitting a continuous jamming signal, or several short jamming pulses. Jamming attacks have been considered under an external threat model, in which the jammer is not part of the network. Under this model, jamming strategies include the continuous or random transmission of high- power interference signals. Adversaries with internal knowledge of protocol specifications and network secrets can launch low-effort jamming attacks that are difficult to detect and counter. The most reliable solution to reduce the impact of such attacks is to detect and localize the source of the attack. We propose two techniques to find out the position of the Jammer; one is where the Jammer is assumed to be having uniform circular impact on the network nodes. Here jamming affected nodes at the border share their knowledge about jamming with next hop neighbors, which further will be collaborated by a chosen monitor node. The other technique implies, two enhanced detection protocols have been used. The first scheme employs the signal strength measurements as a reactive consistency check for poor packet delivery ratio, while the second scheme employs location information to serve as consistency check. Throughout our work we examine the feasibility and effectiveness of our detection scheme. To prevent this attack, a cryptographic scheme SHCS is implemented. It allows safe transmission among the nodes though the jammer is present.

Table of Contents

List of Figures

List of Tables

List of Abbreviations

Abbreviation	Explanation
AONT	All-or-nothing transform
AODV	Ad hoc On-Demand Distance Vector
BN	Border Node
c	Cipher Text
CPHS	Cryptographic Puzzle Hiding Scheme
DSP	Dummy Significant Packet
E_k	Encryption Key
MD5	MD5 was initially designed to be used as a cryptographic hash function, it has been found to suffer from extensive vulnerabilities.
MAC	Media Access Control
PHY	Physical Layer
P	Packet
RN	Receiver Node
RP	Receiver Packet
Rm	Range in meter
SJ	Selective Jamming
SP	Sender Packet
TCP	Transmission Control Protocol
MAC	Media Access Control
PHY	Physical Layer
P	Packet
RN	Receiver Node
RP	Receiver Packet
Rm	Range in meter
SJ	Selective Jamming

Chapter 1

Introduction

The open nature of the wireless medium leaves it vulnerable to intentional interference attacks, typically referred to as jamming. This intentional interference with wireless transmissions can be used as a launch pad for mounting Denial-of-Service attacks on wireless networks. Typically, jamming has been addressed under an external threat model. However, adversaries with internal knowledge of protocol specifications and network secrets can launch low-effort jamming attacks that are difficult to detect and counter. In this work, we address the problem of selective jamming attacks in wireless networks. In these attacks, the adversary is active only for a short period of time, selectively targeting messages of high importance. We illustrate the advantages of selective jamming in terms of network performance degradation and adversary effort by presenting two case studies; a selective attack on TCP and one on routing. We show those selective jamming attacks can be launched by performing real-time packet classification at the physical layer. To mitigate these attacks, we develop three schemes that prevent real-time packet classification by combining cryptographic primitives with physical layer attributes. We analyze the security of our methods and evaluate their computational and communication overhead. Wireless networks rely on the uninterrupted availability of the wireless medium. To interconnect participating nodes. However, the open nature of this medium leaves it vulnerable to multiple security threats. Anyone with a transceiver can eavesdrop on wireless transmissions, inject spurious messages, or jam legitimate ones. While eavesdropping and message injection can be prevented using cryptographic methods, jamming attacks are much harder to counter. They have been shown to actualize severe Denial-of-Service (DoS) attacks against wireless networks. In the simplest form of jamming, the adversary interferes with the reception of messages by transmitting a continuous jamming signal, or several short jamming pulses. Typically, jamming attacks have been considered under an external threat model, in which the jammer is not part of the net-work. Under this model, jamming strategies include the continuous or random transmission of high-power interference signals. However, adopting an "always-on" strategy has several disadvantages. First, the adversary has to expend a significant amount of energy to jam frequency bands of interest. Second, the continuous presence of unusually high interference levels makes this type of attacks easy to detect. Conventional anti-jamming techniques rely extensively on spread-spectrum (SS) communications, or some form of jamming evasion (e.g., frequency hopping, or spatial retreats). SS techniques provide bit-level protection by spreading bits according to a secret pseudo-noise (PN) code, known only to the communicating parties. These methods can only protect wireless transmissions under the external threat model. Potential disclosure of secrets due to node compromise neutralizes the gains of SS. Broadcast communications are particularly vulnerable under an internal threat model because all intended receivers must be aware of the secrets used to protect transmissions. Hence, the compromise of a single receiver is sufficient to reveal relevant cryptographic information. In this paper, we address the problem of jamming under an internal threat model. We consider a sophisticated adversary who is aware of network secrets and the implementation details of network protocols at analyzer in the network stack. The adversary exploits his internal knowledge for launching selective jamming attacks in which specific messages of “high importance” are targeted. For example, a jammer can target route-request/route-reply messages at the routing layer to prevent route discovery, or target TCP acknowledgments in a TCP session to severely degrade the throughput of an end-to-end flow. To launch selective jamming attacks, the adversary must be capable of implementing a “classify-then-jam” strategy before the completion of a wireless transmission. Such strategy can be actualized either by classifying transmitted packets using protocol semantics, or by de-coding packets on the fly. In the latter method, the jammer may decode the first few bits of a packet for recovering useful packet identifiers such as packet type, source and destination address. After classification, the adversary must induce a sufficient number of bit errors so that the packet cannot be recovered at the receiver. Selective jamming requires an intimate knowledge of the physical (PHY) layer, as well as of the specifics of upper layers.

1.1 Jamming Attack

A well-known attack on wireless communication, jamming interferes with the radio frequencies a network’s nodes are using. An adversary can disrupt the entire network with k randomly distributed jamming nodes, putting N nodes out of service, where k is much less than N. For single-frequency networks, this attack is simple and effective. A node can easily distinguish jamming from the failure of its neighbors by determining that constant energy, not lack of response, impedes communication. Both effects have similar results, however, since constant jamming prevents nodes from exchanging data or even reporting the attack to remote monitoring stations.

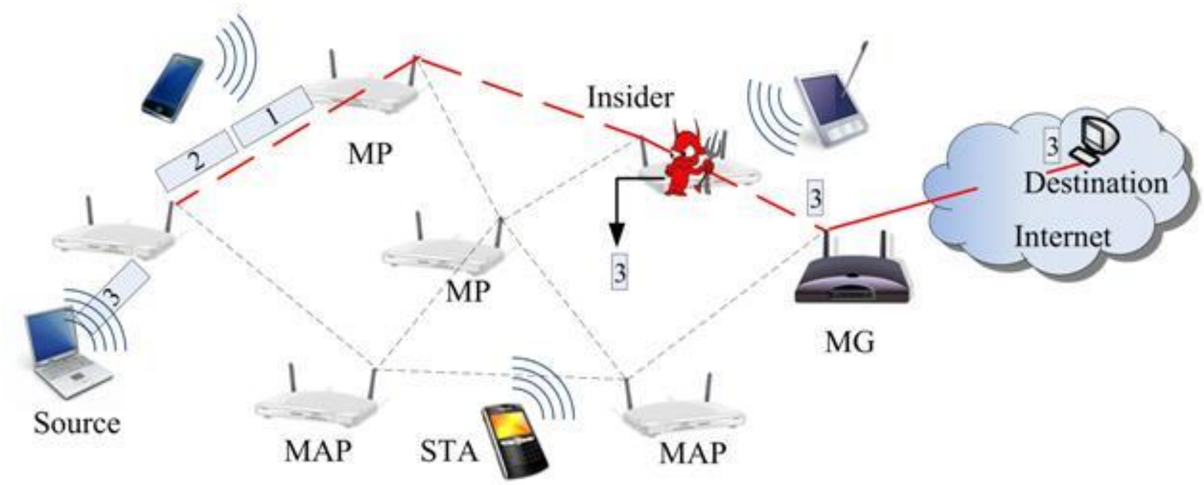


Figure 1.1.1: Jamming Attack

Even sporadic jamming can be enough to cause disruption because the data the network is communicating may be valid for only a short time. The standard defense against jamming involves various forms of spread-spectrum communication. To attack frequency hoppers, jammers must be able either to follow the precise hopping sequence or to jam a wide section of the band.

1.2 Background and Present State of the Problem

Continuous jamming has been used as a denial-of-service (DoS) attack against voice communication since the 1940s [15]. Recently, several alternative jamming strategies have been demonstrated [11], [12], [19], [20]. Xu et. al. categorized jammers into four models, (a) a constant jammer that continuously emits noise, (b) a deceptive jammer that continuously broadcasts fabricated messages or replays old ones, (c) a random jammer that alternates between periods of continuous jamming and inactivity, and (d) a reactive jammer who jams only when transmission activity is detected.

Intelligent attacks which target the transmission of specific packets were presented in [8], [18]. Thuente considered an attacker who infers eminent packet transmissions based on timing information at the MAC layer. Law et. al. considered selective jamming attacks in multi-hop wireless networks, where future transmissions at one hop were inferred from prior transmissions in other hops. However, in both [8], [18], real-time packet classification was considered beyond the capabilities of the adversary.

Selectivity was achieved via inference from the control messages already transmitted. Channel-selective jamming attacks were considered in [4], [17]. It was shown that targeting the control channel reduces the required power for performing a DoS attack by several orders of magnitude. To protect control channel traffic, control information was replicated in multiple channels. The "locations" of the channels where control traffic was broadcasted at any given time, was cryptographically protected. In [9], we proposed a randomized frequency hopping algorithm, to protect the control channel inside jammers.

Finally, P pperoet. al. proposed a frequency hopping anti-jamming technique that does not require the sharing of a secret hopping sequence, between the communicating parties [12].

In Existing System Wireless networks rely on the uninterrupted availability of the wireless medium to interconnect participating nodes. However, the open nature of this medium leaves it vulnerable to multiple security threats. Anyone with a transceiver can eavesdrop on wireless transmissions, inject spurious messages, or jam legitimate ones. While eavesdropping and message injection can be prevented using cryptographic methods, jamming attacks are much harder to counter. They have been shown to actualize severe Denial-of-Service (DoS) attacks against wireless networks.

1.3 Motivation of the Research

At present, in our country, there are only a few researches or publication. This is a concern for our country. To improve in IT sector there is need to improve in security issues and to improve this with effective performance we need a solid defense and greater communication with a perfect efficiency. That is the motivation of the research.

1.4 Objectives

The objectives are given below:

- To investigate the feasibility of real-time packet classification for launching selective jamming attacks considering an internal threat model.
- To analyze the geometric explanation.
- To detect selective jamming attack.
- To analyze the security of our schemes and show strong security with minimal impact on network performance.

1.5 Contribution of the Work

Our key objectives and possible outcomes of this work may mention in the following:

- We proposed a new scheme in which, we will overcome disadvantage of AONT and which also Prevents selective Jamming.
- In this scheme, packets are sending with headers, sequence ID and the Host name and the Data is send directly to the selected host.
- Detects Source or the Jammer.
- Explain with mathematical/geometric properties.

1.6 Challenges

Preventing the jamming node from classifying m in real time, thus mitigating J's ability to perform selective jamming .React at the quickest time after detecting the jammed node. Apply the possible methods to ensure security with minimal performance reduce.

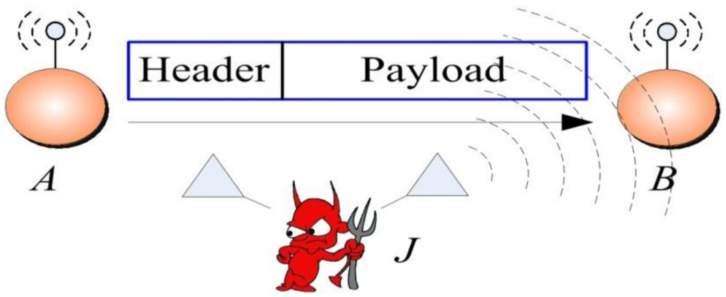


Figure 1.5.1: Jamming Attack [A- Sender Node, B-Receiver Node, J-Jamming Node m-Packets in wireless media transmitted from A to B]

1.7 Organization of the Report

The remainder of the report is structured as follows. In the next chapter, an overview of our project related terminologies, the relation among packet hiding method algorithm and with their parameters and also contains brief discussion on previous works that is already implemented with their limitations. Chapter 3 describes the working procedure of our proposed system. In Chapter 4, we have illustrated our implementation of the project in details. Chapter 5 centers on the experimental result of the proposed system. In order to evaluate the system, we have used subjective as well as quantitative measures. The project concludes with a summary of research contributions and future plan of our work in Chapter 6. This thesis contains two appendices intended for persons who wish to explore certain topics in greater depth. I tried every way to make this research to carry forward to the more advanced system as well.

Chapter 2

Literature Review

In this chapter, we present studies on the terminologies related to the project which are important to understand. This chapter also contains brief discussion on related previous works.

2.1 Jamming Techniques

Jamming makes use of intentional radio interferences to harm wireless communications by keeping communicating medium busy, causing a transmitter to back-off whenever it senses busy wireless medium, or corrupted signal received at receivers. Jamming mostly targets attacks at the physical layer but sometimes cross-layer attacks are possible too. In this section, we elaborate on various types of jammers and the placement of jammers to maximize the jammed area.

2.2 Classification of Jammers

Jammers are malicious wireless nodes planted by an attacker to cause intentional interference in a wireless network. Depending upon the attack strategy, a jammer can either have the same or different capabilities from legitimate nodes in the network which they are attacking. The jamming effect of a jammer depends on its radio transmitter power, location and influence on the network or the targeted node. A jammer may jams a network in various ways to make the jamming as effective as possible. Basically, a jammer can be either elementary or advanced depending upon its functionality. For the elementary jammers, we divided them into two sub-groups: proactive and reactive. The advanced ones are also classified into two sub-types: function-specific and smart-hybrid. The detailed classification of different jammers can be found in Fig. 1.5.1

2.2.1 Proactive jammer

Proactive jammer transmits jamming (interfering) signals whether or not there is data communication in a network. It sends packets or random bits on the channel it is operating on, putting all the others nodes on that channel in non-operating modes. However, it does not switch channels and operates on only one channel until its energy is exhausted. There are three basic types of proactive jammers: constant, deceptive and random. From here on, whenever we use proactive jammers it can mean all these three.

Constant jammer emits continuous, random bits without following the CSMA protocol (Xu et al, 2005). According to the CSMA mechanism, a legitimate node has to sense the status of the wireless medium before transmitting. If the medium is continuously idle for a DCF Inter frame Space (DIFS) duration, only then it is supposed to transmit a frame. If the channel is found busy during the DIFS interval, the station should defer its transmission. A constant jammer prevents legitimate nodes from communicating with each other by causing the wireless media to be constantly busy. This type of attack is energy inefficient and easy to detect but is very easy to launch and can damage network communications to the point that no one can communicate at any time.

Deceptive jammer continuously transmits regular packets (Xu et al, 2005) instead of emitting random bits (as in constant jammer). It deceive other nodes to believe that a legitimate transmission is taking place so that they remain in receiving states until the jammer is turned off or dies. Compared to a constant jammer, it is more difficult to detect a deceptive jammer because it transmits legitimate packets instead of random bits. Similar to the constant jammer, deceptive jammer is also energy inefficient due to the continuous transmission but is very easily implemented.

Random jammer intermittently transmits either random bits or regular packets into networks (Xu et al, 2005). Contrary to the above two jammers, it aims at saving energy. It continuously switches between two states: sleep phase and jamming phase. It sleeps for a certain time of period and then becomes active for jamming before returning back to a sleep state. The sleeping and jamming time periods are either fixed or random. There is a tradeoff between jamming effectiveness and energy saving because it cannot jam during its sleeping period. The ratios between sleeping and jamming time can be manipulated to adjust this tradeoff between efficiency and effectiveness.

2.2.2 Reactive Jammer

Reactive jammer starts jamming only when it observes a network activity occurs on a certain channel (Xu et al, 2005). As a result, a reactive jammer targets on compromising the reception of a message. It can disrupt both small and large sized packets. Since it has to constantly monitor the network, reactive jammer is less energy efficient than random jammer. However, it is much more difficult to detect a reactive jammer than a proactive jammer because the packet delivery ratio (PDR) cannot be determined accurately in practice. According to (Pelechrinis et al, 2011), the following are two different ways to implement a reactive jammer.

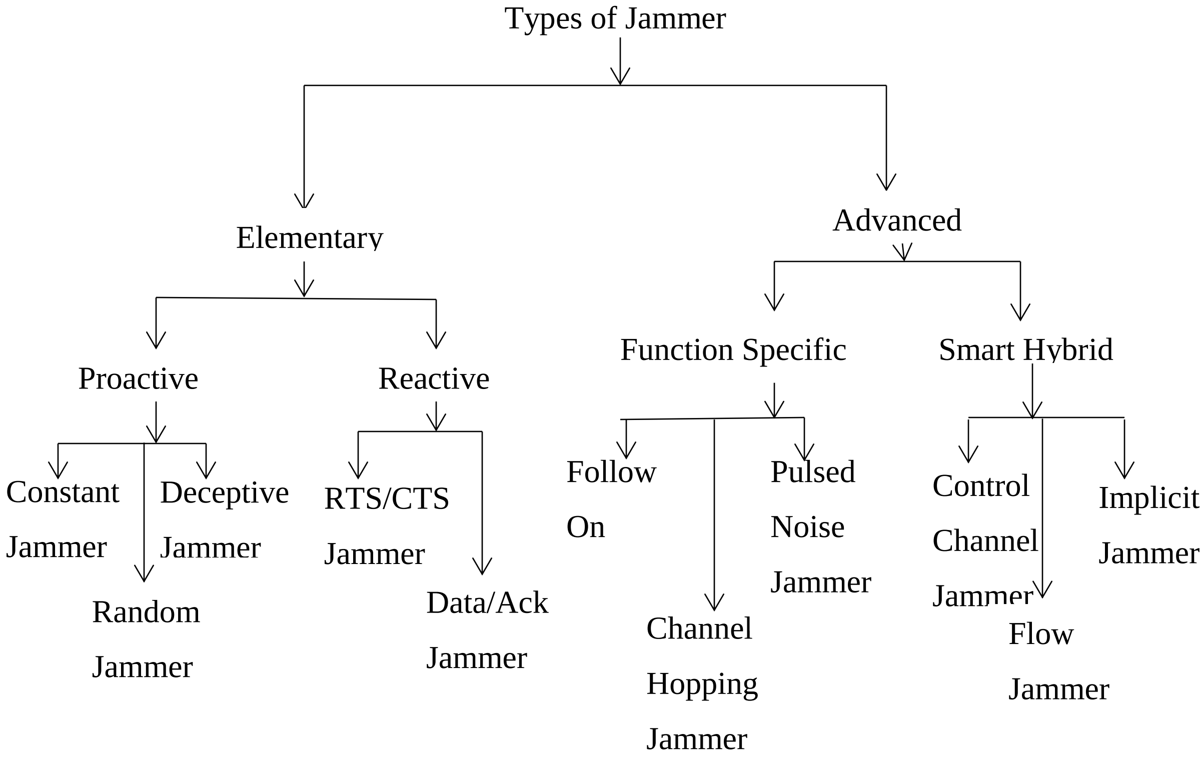


Figure 2.2.2: Types of jammers in wireless networks

Reactive RTS/CTS jammer jams the network when it senses a request-to-send (RTS) message is being transmitted from a sender. It starts jamming the channel as soon as the RTS is sent. In this way, the receiver will not send back clear-to-send (CTS) reply because the RTS packet sent from a sender is distorted. Then, the sender will not send data because it believes the receiver is busy with another on-going transmission. Alternatively, the jammer can wait after the RTS to be received and jams when the CTS is sent by the receiver. That will also result in the sender not sending data and the receiver always waiting for the data packet (Pelechrinis et al, 2011).

Reactive Data/ACK jammer jams the network by corrupting the transmissions of data or acknowledgement (ACK) packets. It does not react until a data transmission starts at the transmitter end. This type of jammer can corrupt data packets, or it waits until the data packets reach the receiver and then corrupts the ACK packets (Pelechrinis et al, 2011). The corruptions of both data packets and ACK messages will lead to re-transmissions at the sender end. In the first case, because the data packets are not received correctly at the receiver, they have to be re-transmitted. In the second case, since the sender does not receive the ACKs, it believes something is wrong at the receiver side, e.g. buffer overflow. Therefore, it will retransmit the data packets.

2.2.3 Function-specific Jammers

Function-specific jamming is implemented by having pre-determined function. In addition to being either proactive or reactive, they can either work on a single channel to conserve energy or jam multiple channels or maximize the jamming throughput irrespective of the energy usage. Even when the jammer is jamming single channel at a time, they are not fixed to that channel and can change their channels according to their specific functionality.

Follow-on jammer hops over all available channels very frequently (thousand times per second) and jams each channel for a short period of time (Mpitziopoulos et al, 2007). If a transmitter detects the jamming and switches its channel, the follow-on jammer will scan the entire band and search for a new frequency to jam again. Or, it may follow a pseudo-random frequency hopping sequence. This type of jammer conserves power by limiting its attack to a single channel before hopping to another. Due to its high frequency hopping rate, the follow-on jammer is particularly effective against some anti-jamming techniques, e.g. frequency hopping spread spectrum (FHSS) which uses a slow-hopping rate.

Channel-hopping jammer hops between different channels proactively (Alnifie and Simon, 2007, 2010). This type of jammer has direct access to channels by overriding the CSMA algorithm provided by the MAC layer. Moreover, it can jam multiple channels at the same time. During its discovery and vertex-coloring phases, the jammer is quiet and is invisible to its neighbors. Then, it starts performing attacks on different channels at different times according to a predetermined pseudo-random sequence.

Pulsed-noise jammer can switch channels and jam on different bandwidths at different periods of time. Similar to the random jammer, pulsed-noise jammer can also save energy by turning off and on according to the schedule it is programmed for. Unlike the elementary proactive random jammer which attacks only one channel, pulsed-noise jammer can attack multiple channels. Moreover, it can be implemented to simultaneously jam multiple channels. (Muraleedharan and Osadciw, 2006).

2.2.4 Smart-hybrid Jammers

We call them smart because of their power efficient and effective jamming nature. The main aim of these jammers is to magnify their jamming effect in the network they intend to jam. Moreover, they also take care of themselves by conserving their energy. They place sufficient energy in the right place so as to hinder the communication bandwidth for the entire network or a major part of the network, in very large networks. Each of this type of jammer can be implemented as both proactive and reactive, hence hybrid.

Control channel jammers work in multi-channel networks by targeting the control channel, or the channel used to coordinate network activity (Lazos et al, 2009). A random jammer that targets the control channel could cause a severe degradation of network performance, while a continuous jammer targeting the control channel might deny access to the network altogether. These attacks are usually accomplished by compromising a node in the network. Furthermore, future control channel locations can be obtained from the compromised nodes.

Implicit jamming attacks are those that in addition to disabling the functionality of the intended target, cause denial-of-service state at other nodes of the network too (Broustis et al, 2009). This attack exploits the rate adaptation algorithm used in wireless networks, where the AP (Access Point) caters to the weak node by reducing its rate. Due to this process, the AP spends more time communicating with this weak node than the other nodes. Therefore, when the implicit attacker jams a node which is communicating with the AP, the rate adaptation effect will increase the AP's focus on the jammed node while causing other clients to suffer.

Flow-jamming attacks involve multiple jammers throughout the network which jams packets to reduce traffic flow. As implemented by Tague et al (2008), these attacks are launched by using information from the network layer. This type of jamming attack is good for the resource-constrained attackers. If there is centralized control, then the minimum power to jam a packet is computed and the jammer acts accordingly. In a non-centralized jammer model, each jammer shares information with neighbor jammers to maximize efficiency.

We summarize the features of all the above-mentioned jamming techniques in Table 1. For every type of jammer, we determine whether it is a proactive or reactive, energy efficient or not, and its ability to jam single channel or multiple channels. However, there are some jamming strategies which combine two or more of these techniques (Bellardo and Savage, 2003). For instance, Wilhelm et al (2011) implement single-tone reactive jamming to generate an optimal jamming strategy by combining the various available forms. Bayraktaroglu et al (2008) use the variations of jammers to analyze the performance of the best jamming strategy in their IEEE 802.11 networks. They experiment with periodic, memoryless jammers based on **Poisson** processes, channel-aware jammers, and omniscient jammers to conclude that channel-aware jammers are the most effective amongst the four types.

In a similar way, Wood et al (2007) use the variations and combination of reactive/random and multi-channel/pulsed-noise jammers to form attacks such as interrupt jamming, scan jamming and pulse jamming. In the interrupt jamming, the jammer stays in sleep states and begins jamming only when it is signaled by the hardware on detection of radio activities. Scan jamming lets the attacker scan each channel first and start jamming if activities are detected. Pulse jamming is the continuously/intermittently jamming on a single channel in which the attacker transmits blindly in short bursts.

2.3 Placement of jammers

In addition to the attacker possessing the above qualities, placement of the jammer plays an important role in effective jamming. Jammers can be placed randomly or can be placed based on a jamming technique which locates the best position to accomplish its objective of jamming with as many nodes as possible. In this section, we will inspect this optimization problem by looking at various placements of jammers.

2.3.1 Optimal jamming attacks

Li et al (2007) show that the probability of jamming can be made high if the attacker is aware of the network-strategy as well as its transmission powers. In addition, the jammer needs to have knowledge about the network channel access probabilities and the number of neighbors to the monitor node (detecting node). All the other nodes in the network just perform the usual IEEE 802.11 simplex communication. The monitor node uses the Sequential Probability Ratio Test for sequential testing between two hypotheses concerning probability of false alarm and probability of missed detection.

The jammers and transmitters/receivers are distributed in a given area using Poisson distribution. The expected values of successful transmission are computed in terms of probabilities. If a particular area is jammed, then the monitor node is expected to send the jamming notification out of the area (using multi-hop transmission); this also suffers from the jamming in the area. Using a probability of distribution and a mathematical proof, the authors proved that the optimal strategy for the attacker tends to be rather mild and long-term.

2.3.2 Jamming under complete uncertainty

Commander et al (2008) use a dynamic approach to compute the location for placing jamming devices by integrating the bounds of the area to be jammed. They assume a square-shaped area encloses the network where the jammers are placed at the intersections of a uniform grid. They formulate the problem as follows. If the jammers have to optimally jam all the nodes of

Table 2.3.2: Types of Jammers

Jammer	Proactive	Reactive	Energy efficient	Single channel	Multiple channels
Constant	×			×	
Deceptive	×			×	
Random	×		×	×	
RTS/CTS jammer		×		×	
Data/ACK jammer		×		×	
Follow-on	×		×	×	
Channel hopping		×		×	×
Pulsed noise	×			×	×
Control channel	×	×	×	×	
Implicit	×	×	×	×	
Flow-jamming	×	×	×	×	×

the network then where should they be placed? Sub-problems are created and solved in order to achieve an optimal result.

They assume that the attacker has limited network knowledge, i.e., the attacker only knows the bounding area, and that the jammers have omnidirectional antennas. They consider that jamming power decreases inversely to the squared distance from a device. Also, the minimum number of jamming devices to jam the complete network is computed in this scheme, given that at any point there is jamming when the total power received at a particular point is greater than the threshold power required to jam the wireless communication.

2.3.3 Limited-range jamming attacks

Jammers with transmission range half that of legitimate nodes can jam the network because the interference range of wireless devices is twice the transmission range (Huang et al, 2010). Contrary to the above schemes this jamming attack does not require global knowledge. Besides, due to the limited transmission range, these jammers are not easily detected. These jammers are placed at strategic locations. Usually the locations are close to the nodes which have the maximum traffic flow (in/out). The authors have shown the experimental results using normal range, limited range and double range (transmission range) jammers.

The normal range jammers have the same transmission range as legitimate nodes; which makes their interference range twice that of the transmission range. Similarly, the limited-range jammers are formed with half the transmission range and hence, interference range equal to the transmission range of the legitimate nodes. Experiments on these jammers in an OPNET simulator show that the detection of these limited-range jammers is difficult because the transmission power is half that of the legitimate nodes. They concluded that limited-range jammers are difficult to detect because they decrease the metrics that are most commonly used for detection, such as SNR and PDR.

2.3.4 DSS for locating VHF/UHF jammer

Gencer et al (2008) defined a jamming system which should be placed at the optimum location such that it completely demolishes the communication capability of the target system. These kinds of systems are usually used by military applications. More number of candidate points or selected points for deploying jammer system is considered in comparison to the target points and the number of jamming systems available. They assume there is line-of-sight between the jammer and target systems, targets are within the antenna range, and the signal power of the jamming system is higher than the signal power of the target system.

The basic purpose of this decision support system is to find or identify the location at which the radio jammer systems should be placed such that it will jam the maximum area possible. Hence, they use the maximum covering model and solve it using the LINGO-8 package. LINGO is an integrated package that includes a powerful language for expressing optimization models. Given the number of target points, candidate points and jamming systems available, the locations for deploying jammers are obtained.

2.3.5 Nano size jammer

Panyim et al (2009) advocates the use of a large number of tiny, low-power jammers that are difficult to detect as they are not visible to the naked eye, being so smaller in size. The implementation of these jammers is in the form of a network. With the total jamming power being constant, they achieve a phase transition of jamming throughput. Reactive jammers are deployed throughout the network.

Experimental results of this paper show that they provide superior performance to traditional jammers. The number of jammers can be increased, thus reducing their jamming power and holding the total power consumed by the jammers constant. They used the scaling behavior of percolation theory. They proved the difficulty in detecting their jammers because of their low-power, small size and high effectiveness in their network formation.

Table 2.3.5: Placement of jammers

Placement strategy	Network Knowledge	Transmission power	Number of jammers	Detection level
Optimal jamming attacks	Yes	Controllable	One	Difficult
Jamming under complete uncertainty	Limited	Calculated	Many	Moderate
Limited-range jamming attacks	No	Low	Many	Difficult
DSS for locating VHF/UHF jammer	Yes	High	Many	Easy
Nano Size Jammer	No	Low	Many	Very difficult

In summary, these five jammer placement strategies are analyzed in Table 2 where we investigate if network knowledge is required, the transmission power of jammers, the number of jammers and the difficulty in being detected.

2.4 Detection techniques

2.4.1 Detection of Denial of Sleep Attack

In denial of Sleep attack adversary is knowledge of MAC layer protocol and ability to bypass authentication and encryption protocols.MAC layer protocol designed for wireless sensor network and use various algorithm to save battery power by placing radio in low power mode. In this paper divide MAC protocol in four types i.e. Sensor MAC(S-MAC), Timeout MAC (T-MAC), Berkeley MAC (B-MAC), and Gateway MAC (G-MAC).We analyze all these MAC protocol in detail as follows:

S-MAC frame is divided in to listening and Sleep period. The listening period is divided in to synchronization and transfer period. In Synchronization period all the nodes announce their sleep schedule for correcting network time out. Synchronization their sleep time to form virtual cluster with the same active listen and sleep period. It is used

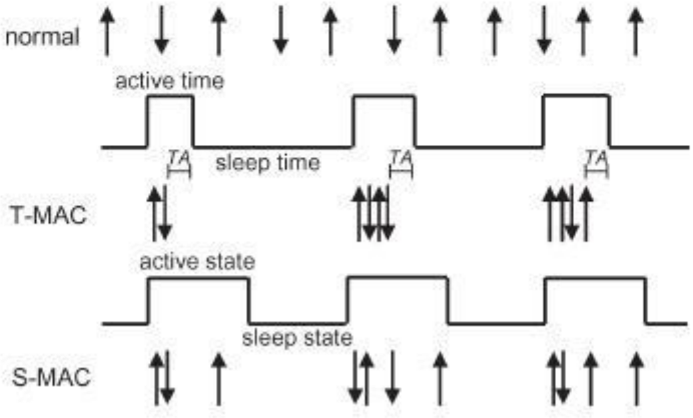


Figure 2.4.1: T-MAC adaptive timeout

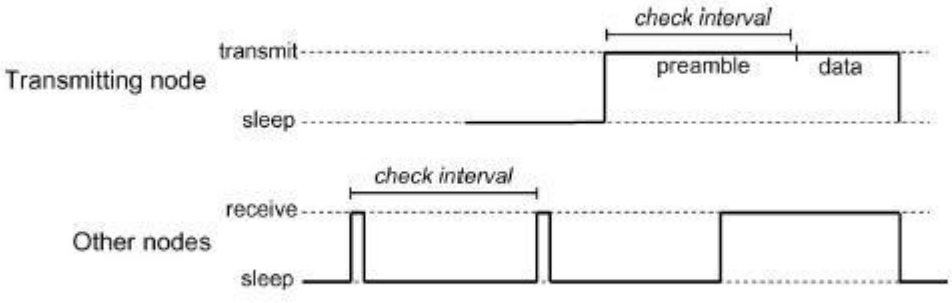


Figure 2.4.2: B-MAC low power listening

fixed duty cycle with a default 10%.If a node overhears two SYNC messages, it will adapt both duty cycles to maintain network and enhance network lifetimes. T-MAC is an improvement in the S-MAC protocol by concentrating all traffic at the beginning of the duty period, as shown in Figure 2.4.2 The arrows in the figure indicate transmitted and received messages. T-MAC uses the same SYNC mechanism to form virtual clusters as S-MAC.T-MAC uses adaptive timeout (TA) mechanism allows nodes to transition to sleep mode when there is no more traffic in the cluster. T-MAC is shown to increase in network lifetime over S-MAC.B-MAC is does not attempt to synchronize sleep schedules. B-MAC uses the low-power listening (LPL) to reduce the energy consumption. In LPL node is walk for fixed interval and check wireless sensor network for valid preamble byte that indicate the pending data transmission of another node. A node sends the pending data and preamble. If it is longer than interval between receiver samples to ensure that all near nodes have the opportunity to receive the preamble and subsequent data message.

In denial-of-sleep attack adversary broadcasting unauthenticated traffic into the network. This unauthenticated traffic reduces network lifetime of the node which uses S-MAC and T-MAC protocol. To enhance network lifetime use G-MAC protocol. In G-MAC protocol requests to broadcast traffic must be authenticated by the gateway node before the traffic can be sent to other nodes. Therefore, only the gateway suffers power loss due to unauthenticated broadcast.

2.4.2 Detection of Path Based DOS attack

In this path based DOS attack is launched by flooding data packet along multi hop end to end path. To defend against path based DOS attack an intermediate node must able to detect spurious packet or replayed packet and then reject them. For the detection of spurious packet use lightweight secure mechanism to defend against path based DOS attack. in this mechanism configures one way hash chain along a path enabling each intermediate node to detect a Path based DOS attack and prevent propagation of spurious or replayed packet. Every packet sent by end point includes new one way hash chain number which is used for message authentication. Different hash chain number is used for each time slot and intermediate node forward packet only if new hash chain number is verified. this process of verification by each intermediate node is continue and each time slot it verify new hash chain number. if number is not validate then the drop the packet.

2.4.3 Detection of Jamming attack

In jamming attack adversary attack in the network under external and internal threat model. In the external threat model jammer is not part of the network. In external model jammer is continuously or randomly transmits high power interference signals. For the prevention of jamming attack from external jammer spread-spectrum communications technique used. Spread Spectrum techniques provide bit-level protection by spreading bits according to a secret pseudo noise (PN) code known only to the communicating parties. These methods can only protect wireless transmissions under the external threat model. In the jamming under internal thread model any sophisticated adversary who is knowledge of network protocol can launch selective jamming attack. To launch selective jamming attack adversary must be capable of implementing “classify then jam” strategy before completion of wireless transmission. After classification, the adversary must introduce a sufficient number of bit errors so that the packet cannot be recovered at the receiver. For the prevention of jamming attack from internal thread model use

packet hiding method. In packet hiding method before classification of the packet by adversary we hide the packets. Hence adversary can’t add bit error in to the packet and it is securely transmits. For the packet hiding method use commitment methods and cryptographic puzzle. In commitment method sender commits the packet and it is verify by the verifier. In the cryptographic puzzle packet m is encrypted with a randomly selected symmetric key k of a desirable lengths. The key k is blinded using a cryptographic puzzle and sent to the receiver. For adversary, the puzzle carrying k cannot be solved before the transmission of the encrypted version of m is completed and the puzzle is received. Hence, the adversary cannot classify m for the purpose of selective jamming.

2.4.4 Detection of wormhole attack

Packet leash is used for detection of wormhole attack. In packet leash sender node uses temporal packet leash and geographical packet leash. In temporal packet leash sender node uses its timestamp i.e. sending time of the packet.

In geographical packet leash sender uses its location and sending time of the packet to receiver. Based on this information receiver estimates distance between sender and receiver. If the estimated distance is longer than the possible radio range, receiver will reject the communication with Sender node.

2.4.5 Detection of Vampire attack

In this Vampire attack can be prevent by using energy weight monitoring algorithm(EWMA).In this algorithm energy of the node is consider for find out threshold level of the node. for find out malicious node in the network every node is add the test field while receiving the packet and forward packet to next node. then test field is check for each node. if the test field is correct then normal operation is continue and if the test field is wrong then create an alarm packet. then alarm packet is broadcast and announce that node is malicious so that it avoid for further communication. That malicious node reaches its threshold level. This algorithm is divided in two phases such as communication phase and network configuring phase. In network configuring phase establish optimum routing path from source to destination. Attacked node consumes more energy and reaches threshold energy level. In this phase the node with threshold level energy (attacked node) sends ENG_WEG message to all its surrounding nodes. After receiving the ENG_WEG packets the surrounding nodes sends the ENG_REP message that encapsulates information regarding their geographical position and current energy level. The node upon receiving this stored in its routing table to facilitate further computations. Now the node is establishes the routing path from source to destination. The source nodes select the node which is less distance from source and require minimum energy to transmit the packet. In communication phase avoid same data packet transmitted repeatedly through same node. These repeatedly transmission of same packet through same node depletes more battery power of the node and degrade the network performance. The process of repeating the packet is eliminated by aggregating the data transmitting within forwarding node. In data aggregation copy the content of the packet which is transmitting through the node. This copied content compare with the data packet transmitting through the node. If the transmitted packet is same as the copied packet then stop the packet transmitted through them. In this way it avoids the redundant packet transmitting through the same node and protect from the vampire attack.

Chapter 3

Methodology

3.1 Proposed System

In Proposed System, we address the problem of jamming under an internal threat model. We consider a sophisticated adversary who is aware of network secrets and the implementation details of network protocols at any layer in the network stack. The adversary exploits his internal knowledge for launching selective jamming attacks in which specific messages of "high importance" are targeted.

To launch selective jamming attacks, the adversary must be capable of implementing a "classify-then-jam" strategy before the completion of a wireless transmission. Such strategy can be actualized either by classifying transmitted packets using protocol semantics, or by decoding packets on the fly.

To mitigate such attacks, we develop three schemes that prevent classification of transmitted packets in real time. Our schemes rely on the joint consideration of cryptographic mechanisms with PHY-layer attributes. We analyze the security of our schemes and show that they achieve strong security properties, with minimal impact on the network performance.

To detect the jammer we combined the geometric approach method with SHCS approach to increase efficiency in reaction.

3.2 Detection of Selective Jamming Attack

If selective jamming is achieved by the adversary for a packet then receiver cannot recover that packet. SJ is just like a normal node but has more computational capabilities than other nodes. We show this SJ node detection in two steps:

(1) Initially, we confirm whether there is a presence of selective jamming between specific SN and RN. If there is selective jamming, we will go for the next step:

(2) Identifying the exact node that is performing selective jamming. The corresponding procedures of these two steps are shown in the following subsections (A and B)

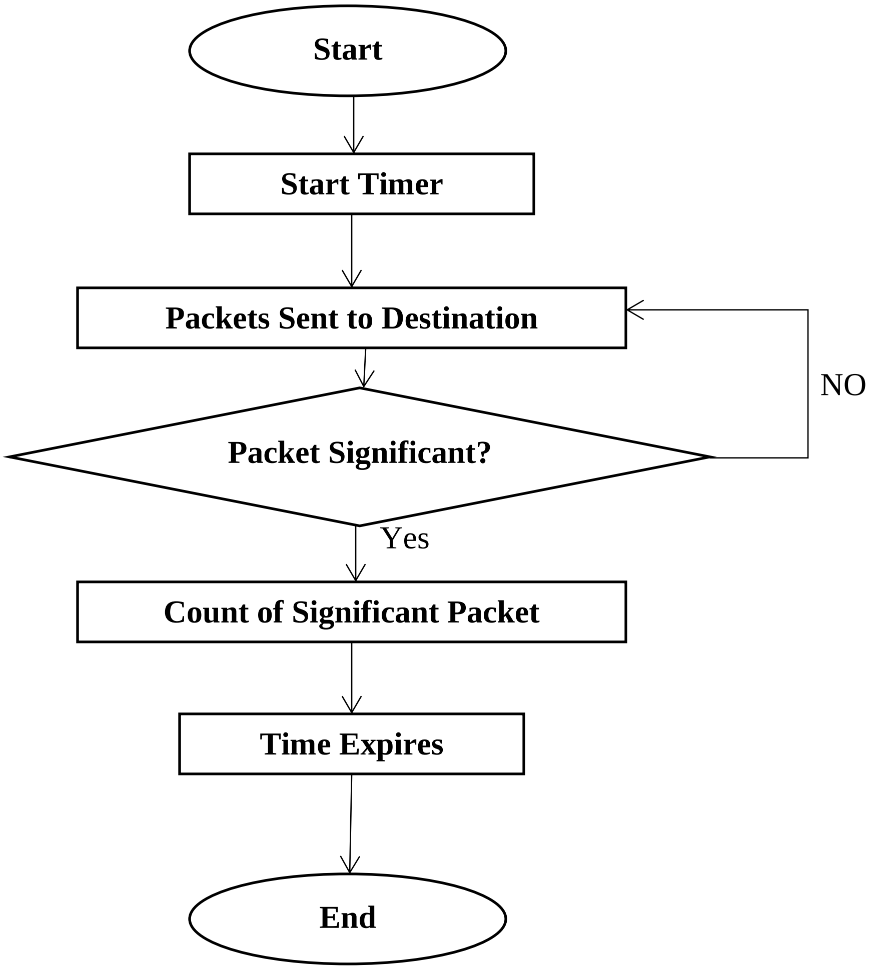


Figure 3.2: Detection of selective jamming

3.2.1 Checking the Existence of Selective Jammer

As shown in Figure 3.2.1, SJ has targeted on SN and RN which classifies each and every packet sent by SN to RN but it only corrupts the significant packets (SP). It will not do any harm to the insignificant packets (IP). The reason behind this is, corrupting only the significant packets would create more bad impact on SN and RN rather than corrupting all.

There is a best existing method called as Packet Delivery Ratio (PDR) with consistency checks [1], which is used to detect various types of Jamming in wireless networks. We have just used the basic idea behind this and proposed a novel approach for the detection of selective jamming. Since, SJ will corrupt all the significant packets leaving the insignificant ones, the number of significant packets that are recovered at RN are zero. During significant synchronization time (T_{ss}), SN will maintain a count of both significant Packets $(CSP)_{SN}$

and insignificant packets $(CIP)_{SN}$,which are later used by it to know SJ node existence(As shown in Algorithm 1). Moreover, RN will also maintain the count of received significant and insignificant packets from SN i.e. $(CSP)_{RN}$ and $(CIP)_{RN}$, during T_{ss}, Where T_{ss} is used by the SN and RN to find whether they are under selective jamming or not.

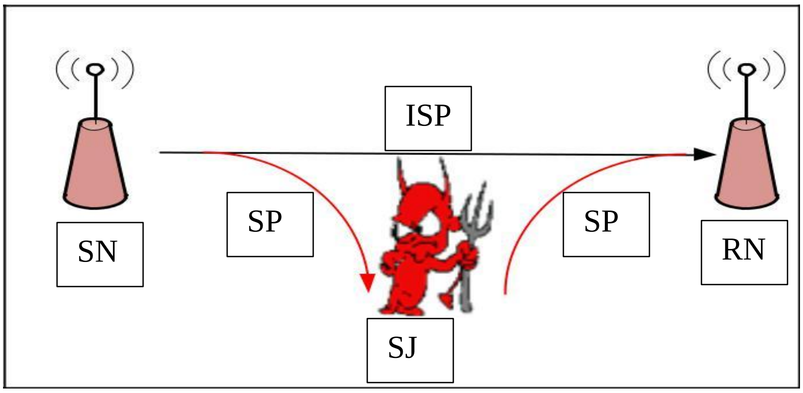


Figure 3.2.1: Selective Jamming Attack

Algorithm 1: Maintaining Count at Sender Node

```
1:  $(CSP)_{SN}$=0,$(CIP)_{SN}$=0;
2:  sendToDest();
3:  startTimer($T_{ss}$);
4:  if $P_i$==SP    // if packet is significant
5:      $(CSP)_{SN}$ ++;
6:  else
7:      $(CIP)_{SN}$++;
8:  end if
9:  Goto (2) and repeat until timer expires;
10: Wait($t\alpha^{);}$
```

We assume that, during T_{ss}, SN will send at least one significant packet and one or more insignificant packets to RN. The time T_{ss} should be synchronized between SN and RN to the maximum extent as possible. To achieve this, SN just starts its T_{ss} after sending its first packet; similarly, RN Starts its T_{ss} after receiving first packet. Initially, SN has started its T_{ss}. This makes T_{ss} at SN to expire first then it waits for some time **tα'**so that it may receive complaints from RN if any.

The SN that receives these values ($(CSP)_{RN}$, $(CIP)_{RN}$ will compare with its (($CSP)_{SN}$ and $(CIP)_{SN}$) values. Then this result will meet any of the possible cases shown below:

ALGO

Case-1: More difference in CSP values of (SN, RN) but very less difference in CIP values of (SN, RN) indicates, there is Selective Jamming between SN and RN, because RN received only insignificant but not significant Packets (SP). (As already shown in Figure 3.2.1).

Case- 2: More difference in both CSP and CIP values of (SN, RN) reveals two possible alternatives a) In Figure 3.3.9.1, SN and RN are under continues jamming because continues Jammer sends high interference signals constantly. So, this makes both SP and IP packets not to reach RN. b) As shown in Figure 3.9.3.2, there may be a presence of poor wireless link between SN and RN. But, there is no presence of Selective Jammer.

Case-3: As depicted in Fig. 3..3.9.3, less difference in CSP values of (SN, RN) but more difference in CIP values of (SN, RN) indicates random jamming (RJ). Random jammer node jams only for some time t_j and for the remaining time it will be in sleep mode. Moreover, RJ do not perform any packet classification which makes it to jam more number of IP than SP. That is, blindly it jams the packets which makes it to show variation in the count results and may even fall in other cases.

Case-4: As depicted in Fig. 3.3.9.4, less difference in both CSP and CIP values of (SN, RN) indicates no jamming. If the total number of packets transmitted by SN is Pn+α· But, say RN received P_n packets. Due to unreliability nature of Wireless network, α packets were unable to reach RN, Where α is very less. Hence no Jamming exists over here. If CSP and CIP values of SN and RN are matched then also it indicates, there was no presence of jammer.

3.3 Block Diagram of preventing Selective Jamming Attack

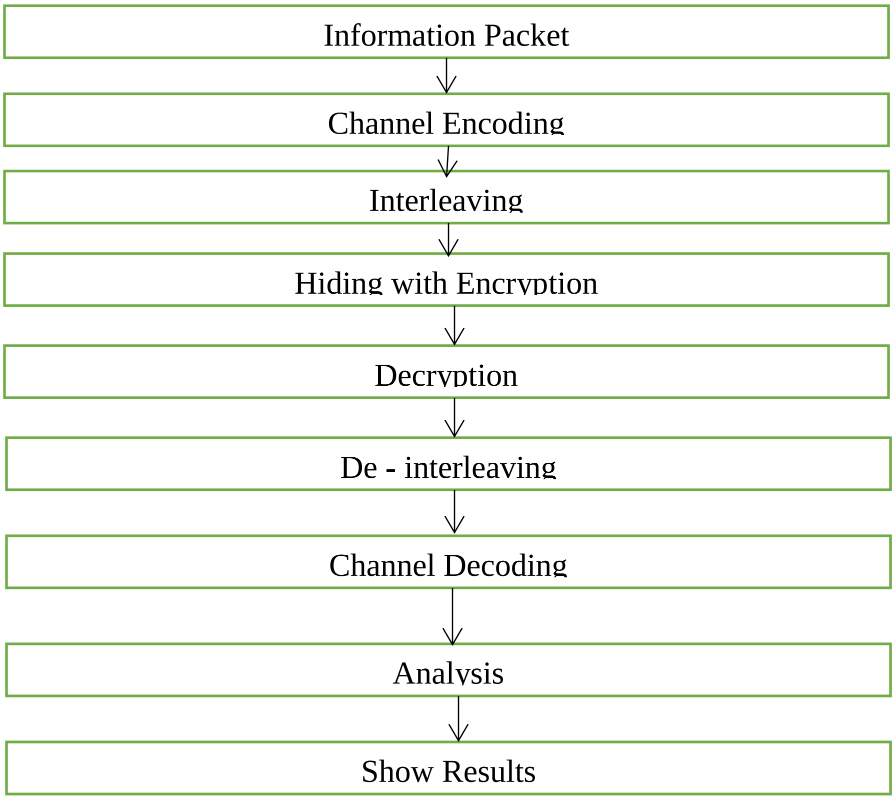


Figure 3.3: Block Diagram of Jamming Attack Prevention

In order to implement the method we have to consider four major modules. They are : -

(1) Network Module

(2) Real Time Packet Classification Module

(3) Packet Hiding Techniques

(4) Selective Jamming Module

(5) Strong Hiding Commitment Scheme(SHCS)

3.3.1 Network module

The network consists of a collection of nodes connected by wireless links. The nodes can communicate directly if they are within communication range, or indirectly through multiple hops. The nodes communicate both unicast mode and broadcast mode. If there is no jammer unencrypted communication performed otherwise encrypted communications performed. For encrypted broadcast communications, packet will send after applying packet hiding method.

3.3.2 Real Time Packet Classification

At the physical layer, a packet m is coded, interleaved and modulated before transmission via the wireless channel. At the receiver, the signal is demodulated, de-interlacing and decryption to recover the original packet m. The nodes A and B communicate via a wireless link. Within the communication range of A and B there is a jamming node J. When A transmits a packet to B m, m classifies the node J receiving only the first bytes of m. J m then corrupted beyond recovery by interfering with their reception at B. Consider the generic communication system shown in FIG. 3.3.2 In the PHY layer, a packet m is coded, interleaved and modulated before transmission via the wireless channel. At the receiver, the signal is demodulated, de-interleaved and decoded to recover the original packet m.

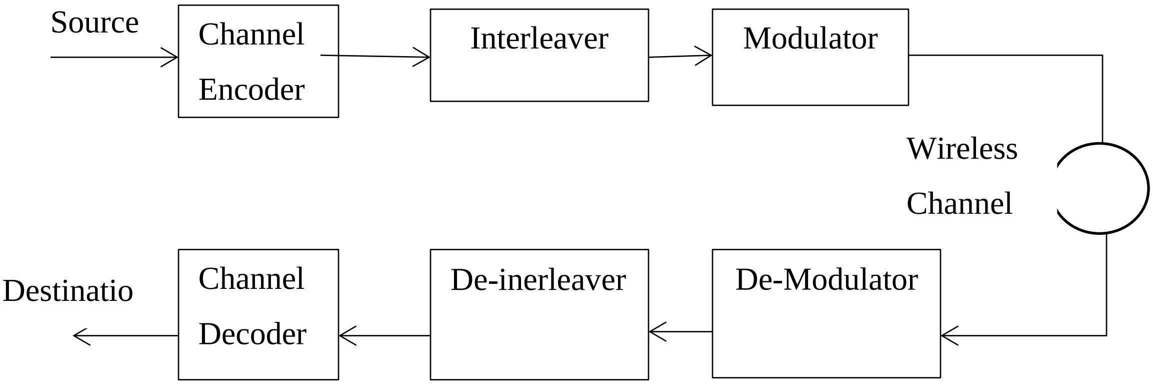


Figure 3.3.2.: Real Time Packet Classification

Moreover, even if the encryption key concealment scheme be kept secret, the static parts of a packet transmitted could potentially lead to packet classification. This is because for computationally efficient methods such as block cipher encryption, the encryption of a plaintext with the same key code you get a text prefix static encryption. Thus, an adversary who is aware of the details of the underlying protocols (frame structure) can use the static text portions of a packet transmitted to classify encryption.

3.3.2.1 System Architecture

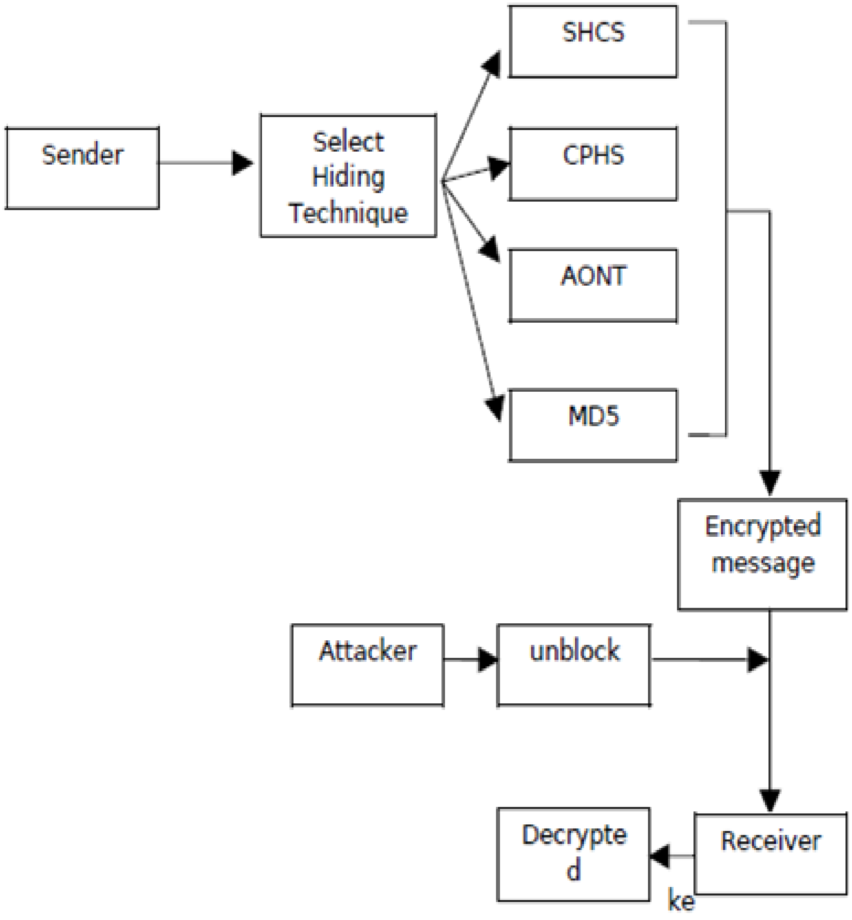


Figure 3.3.2.1: System Architecture

3.3.2.2 Flow Chart

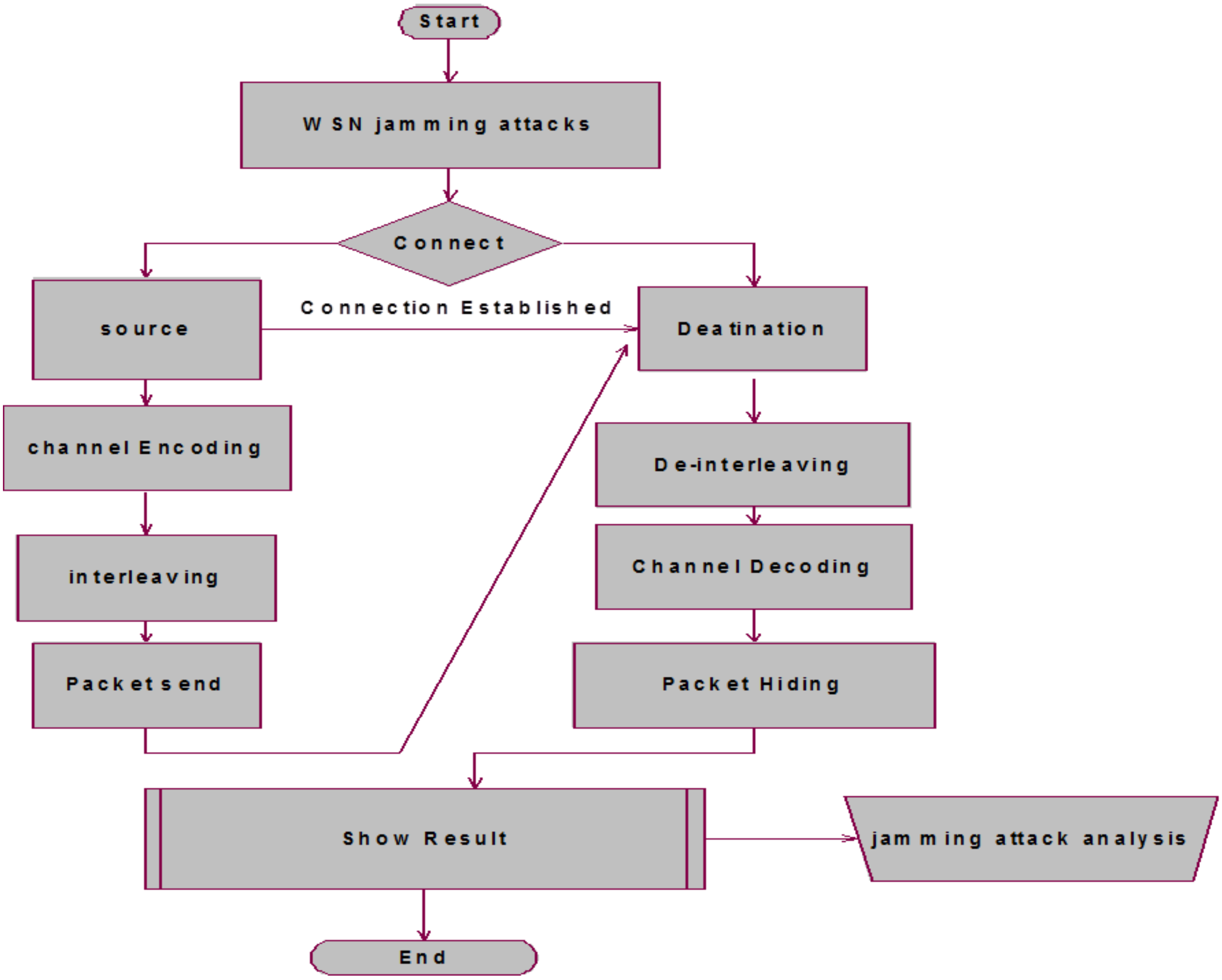


Figure 3.3.2.2 : Flow Chart of Jamming Attack Analysis

3.3.3 Packet Hiding Techniques

In this Module, packet-hiding techniques on the network performance via extensive simulations. To implement the hiding sub layer and measure its impact on the effective throughput of end-to-end connections and on the route discovery process in wireless ad-hoc networks. We chose a set of nodes running 802.11b at the PHY and MAC layers, AODV for route discovery, and TCP at the transport layer. Aside from our methods, we also implemented a simple MAC layer encryption with a static key. We encrypt the serial key of the packet not the message.

These packet-hiding methods require the processing of each individual packet by the hiding sub layer. We emphasize that the incurred processing delay is acceptable, even for real time applications. The SCHS requires the application of two permutations and one symmetric encryption at the sender, while the inverse operations have to be performed at the receiver.

3.3.4 Selective Jamming Module

We illustrate the impact of selective jamming attacks on the network performance. Implement selective jamming attacks in two multi- hop wireless network scenarios. In the first scenario, the attacker targeted a TCP connection established over a multi-hop wireless route. In the second scenario, the jammer targeted network layer control messages transmitted during the route establishment process selective jamming would be the encryption of transmitted packets with a static key. However, for broadcast communications, this static decryption key must be known to all intended receivers and hence, is susceptible to compromise. An adversary in possession of the decryption key can start decrypting as early as the reception of the first cipher text block.

3.3.5 Strong Hiding Commitment Scheme

In this Module, We propose a strong hiding commitment scheme (SHCS), which is based on symmetric cryptography. To satisfy the strong hiding property while keeping the computation and communication overhead to a minimum. To satisfy the strong hiding property, the packet carrying d is formatted so that all bits *of* d are modulated in the last few PHY layer symbols of the packet. To recover d, any receiver must receive and decode the last symbols of the transmitted packet, thus preventing early disclosure of d. We now present the implementation details of SHCS.

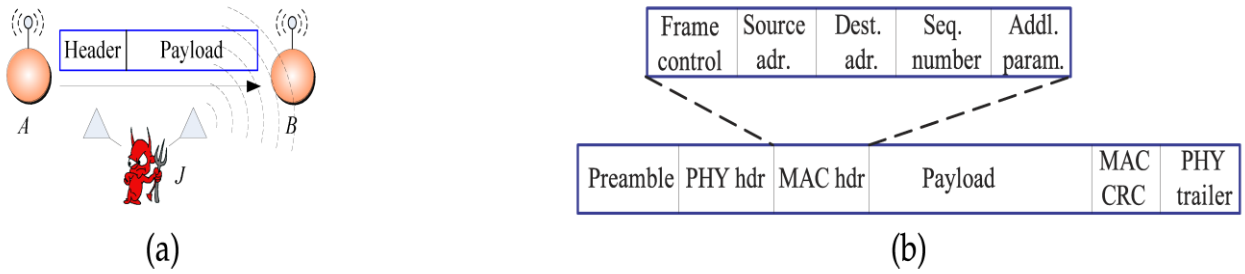


Figure 3.2.1 : Case (a) and (b)

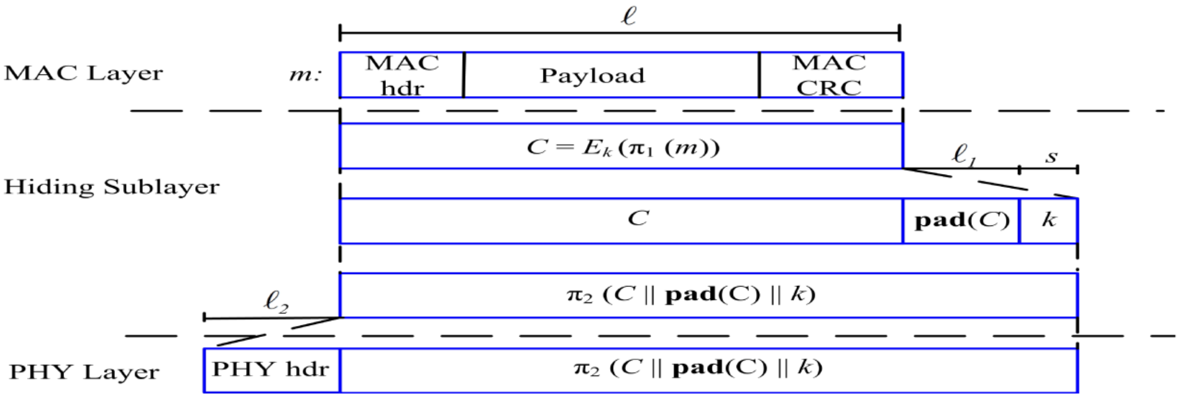


Figure 3.2.1 : PHY Layer, MAC Layer and Hiding Sublayer architecture

3.3.6 SHCS implementation

The Sender's has packet 'P' for receiver 'r'. The implementation of Strong Hiding Commitment Scheme technique has following steps;

I. First apply a permutation of packet 'P'. i.e. $\pi 1$ (P)

II. Encrypt the permutation packet $\pi 1$ (P) with static key 'k' except destination part. The commitment value, c = $E_k(\pi 1$ (P)).

III. The sender broadcast commitment value along with static key 'k'.

IV. At the receiver side, the reverse of above steps will take place.

3.3.7 Wormhole implementation

Wormhole can be used as a reactive defense mechanism. After receiving repeated acknowledgements, the source becomes the wormhole and sends the information regarding the jammer to all other nodes. This wormhole, then prevent the jamming activity of particular jammer. By this method, all other nodes within that network can understand the information about the jammer.

3.3.8 Shortest Path Implementation

Using the communication ranges between nodes, the shortest distance is calculated. A routing table is maintained to store the distance between nodes in a network. Updates are possible to the table whenever necessary.

3.3.9 Finding the Jammer

By using above cases, one can predict whether there is selective jamming between SN and RN or not. If confirmed, SN has to detect the node which is performing selective jamming. Since there are number of nodes between SN and RN, it is not an easy task to accomplish this detection. But, we resolve this by considering the weakness of SJ node. The solution is, SN simply broadcast the HELLO packet when SJ is busy such that it should not answer the HELLO packet but all the free nodes reply immediately. Since, SN does not know the state of SJ, it intentionally sends dummy significant packet (DSP) to RN by puzzling with computational capability more than that of SJ and this makes SJ to take the DSP and will be busy in solving that. The same DSP will reach the Receiver RN but it should not spend time and waste its energy in solving the dummy packet.

So, we can place a restriction as if once complaint is passed by RN to SN, it should not receive any packets directly from SN until there was no selective jamming between SN and RN. DSP means it contains significant data but it is generated randomly by SN and not useful for RN.

The reply from the nodes indicates that they are free nodes (FN) and the nodes which do not reply immediately are treated as Busy Nodes (BN). By using (1), we can find the selective jammer.

Initially, we assume all the nodes within the range of SN and RN as busy Nodes (BN). On just before sending the HELLO packet, intentionally SN makes SJ node to be in busy state, making it not to respond with the packet immediately. So, we treat the nodes that replied quickly as free nodes. Hence, SJ will not be in free nodes list.

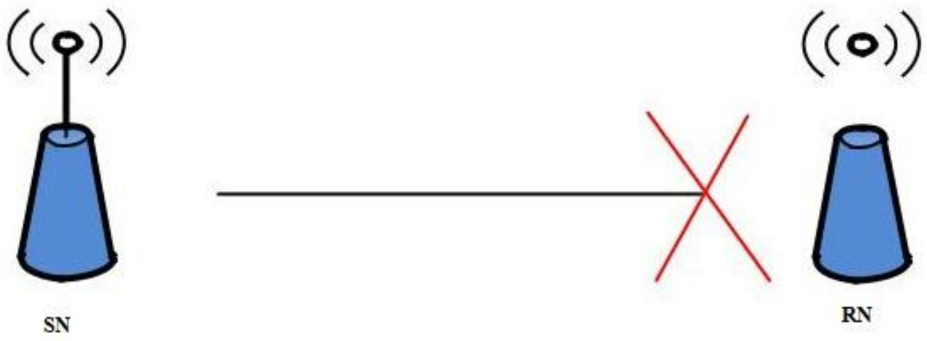


Figure 3.3.9.1: Poor Wireless link

For example, if there are five nodes within the communication range of SN and RN.

Initially, SN sends a DSP to RN, if selective Jammer node is in between SN and RN, then the DSP packet will be taken by SJ and will be busy in solving dummy packet. At that point of time, SN broadcasts HELLO packet and the nodes that are free will reply immediately.

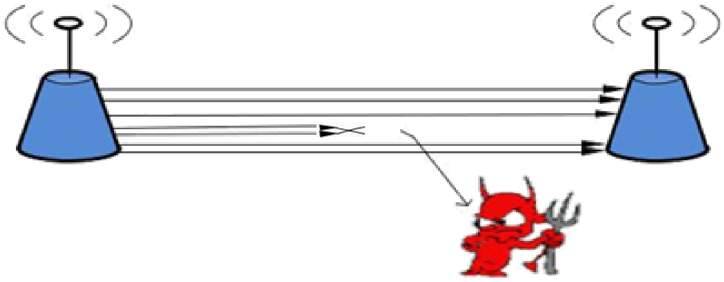


Figure 3.3.9.2: Random Jamming

If the replied nodes are X, Z and Q; by using (1), BN= {X, Y, Z, P, Q}-{X, Z, Q} =>{Y, P}.Among Y and P, one is the selective jammer node. To know this, SN sends another DSP to RN which makes selective jammer to spend time on the DSP. Immediately, SN broadcasts the HELLO packet. Then the nodes which are free currently will reply immediately. If the replied node is {Y}; Then, by using (1), BN={Y, P} – {Y} =>{P}; here „P‟ is the selective jammer (SJ) between SN and RN. Finally, the node in the singleton set is the selective jammer node.

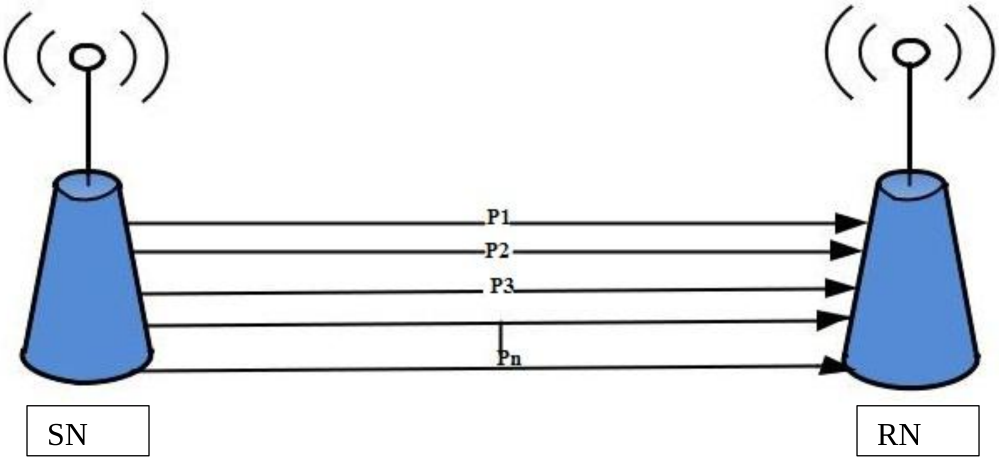


Figure 3.3.9.3: No Selective Jamming

To better confirm the node in singleton set is SJ, we repeat the same for μ number of iterations. This scheme works because a node which may be free during first HELLO packet may not be free during second or third and so on. Thus detection of Jammer may be time taken but ultimately we are detecting the culprit.

3.3.9.1 Finding the Jammer (Geometric Approach)

We make few assumptions about the Network. Every node in the network knows their position co-ordinates with reference to a chosen monitor node. i.e. every node knows its x-axis and y-axis co-ordinates from a reference node. It is assumed that nodes will not change their position without prior notice to the monitor node. i.e. Node remains static in its position. In case it needs to change the position, it informs its new position co-ordinates to the monitor node. Based on the impact of jamming on the nodes, jammed nodes are categorized into three types as: Jammed Node, Border Node and Unaffected Node. The jammer node is assumed to be having Isotropic impact on the nodes of the network. That is in all the directions Jammer will have uniform impact of jamming, with circular sensing range Rms and adaptable transmission range Rm, realized by controlling transmission power Pm. The jammer also controls the probability q of jamming the area within its transmission range, which can be represented by a circle with the jammer as the Centre and its effective jamming distance as the radius.

So as to accomplish the objective, First we need to obtain the set of jammed border nodes. Next is to anticipate the position of the Jammer by collaborating above information and then applying few analytical mathematical formulae and structures to deduce the co-ordinates of the Jammer.

Obtaining Jammed nodes at the Border

A Border node is the node which suffers from jamming attack, but is still able to receive the signals, and its next hop node is a Unaffected node. Such Border nodes transmit a packet saying he's jammed, along with his position co-ordinates to all its neighbors. Further neighbors forward the same packet to a chosen monitor node; usually will be a node with maximum remaining battery.

So the monitor node will get a list of the Border nodes {b1,b2,...,bn}, along with all their node Ids and their positions{x1y1,x2y2,…,xnyn}.

Calculating position of the Jammer:

Having obtained details about border nodes, next task is to finding position of Jammer. It involve set of operations involved- To begin with, the monitor node will first calculate the distance between all border node pairs, (bi, bj), for all i,j<=n Of all pairs, the pair with maximum distance gap is chosen, say (bx, by); Calculate midpoint of line joining (bx,by), say O. Since the Jammer node has circular effect, O is assumed to be the center of the jamming circle caused by the jammer. Next monitor node checks whether the circle with O as center and (bx,by)

Step 2: Else if some node, say bz is outside the circle, then it'll calculate the distance of every border node set from the diameter of the circle. Choose the maximum amongst them as, say bu.

Step 3: Now find perpendicular bisectors of ∆bxbybu, say C.

Step 4: Now check if the Circle with C as Centre and (C,bu) as radius covers the position of the Jammer. Else above procedure is repeated considering the node that lies outside circle from Step 2 till all the nodes lie in the circle.

Analysis of Proposed Work:

To analyze the above proposed methodology, let us consider diagrams 1(a) and 1(b). Suppose that AB be the chord of the circle, Point C lies on the circle and Point D lies outside circle.

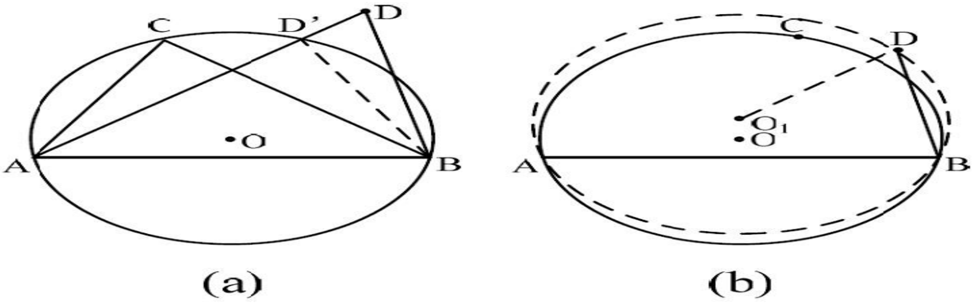


Figure 3.3.8.1 case 1(a), case 2 (b)

Suppose that the line AD intersects circle at D'. On connecting D' to B, it can be seen that ∟ACB=∟AD'B. Since ∟ADB=∟ADB+∟D'BD, it proves that ∟ACB >∟ADB.

Next we draw a circum-circle of ΔABD with center as O1. Now is C has to lie within the circle. Because if it lies outside the circle it means that ∟ACB > ∟ADB is proven false, which is a contradiction. Hence jammer position should be the midpoint of the line joining the nodes separated by maximum distance that covers all the jammed nodes in its circum-circle.

Chapter 4

Implementation

The proposed method is simulated by creating a virtual network using Java Thread API. Each node is created using as separate thread, it is possible to assign each node its position, auto IP assignment, routing table updating. Java.awt.graphics,javax. Swing color packages are used for creating the environments. A jammer node is created using thread and graphics packages for applying selective jamming. A node can be repositioned to any location. A wormhole is generated automatically to migrate from one place to another using graphics API. An alarm is generated by the wormhole as packet to every node in the region

4.1 Implementation Tools

The necessary tools to implement this system can be divided in to Categories-Hardware & Software as illustrated below:

- **Hardware Requirements**
  - Personal Computer
  - System : Pentium IV 2.4 GHz.
  - Hard Disk : 40 GB.
  - Ram : 512 Mb.

- **System Configuration**
    - Personal Computer
    - Operating system : Windows XP/7/8.1
    - Coding Language : JAVA(JAVA Swing, RMI, Eclipse)
    - Internet
    - Paper
- **Software Tools and Libraries**
  - NetBeans IDE

4.2 Requirement of the Problem Analysis

Analysis of packet hiding methods here in this project there are three types of transferring data are performed. First of all I have analyzed the packet size which is transferred to the destination manually. Also calculated the encryption time of different files with different methods. To protect the system from unauthorized access we need to define the network security into following needs:

- Protect the information from accidental, unwanted or unauthorized editing.
- Make a secured delivery to the destination and protect the information.

4.3 Problem Design Input

In this project taken a text file is taken as an input to the system. This file should reach to the destination from source and required processes are performed within intermediate time and data packets safely. We can define this process with geometric approach and find the affected node accurately. Time, Safety and detection is the main research things in this research. The destination must receive the data packets from its source without losing any data.

4.4 Design Details

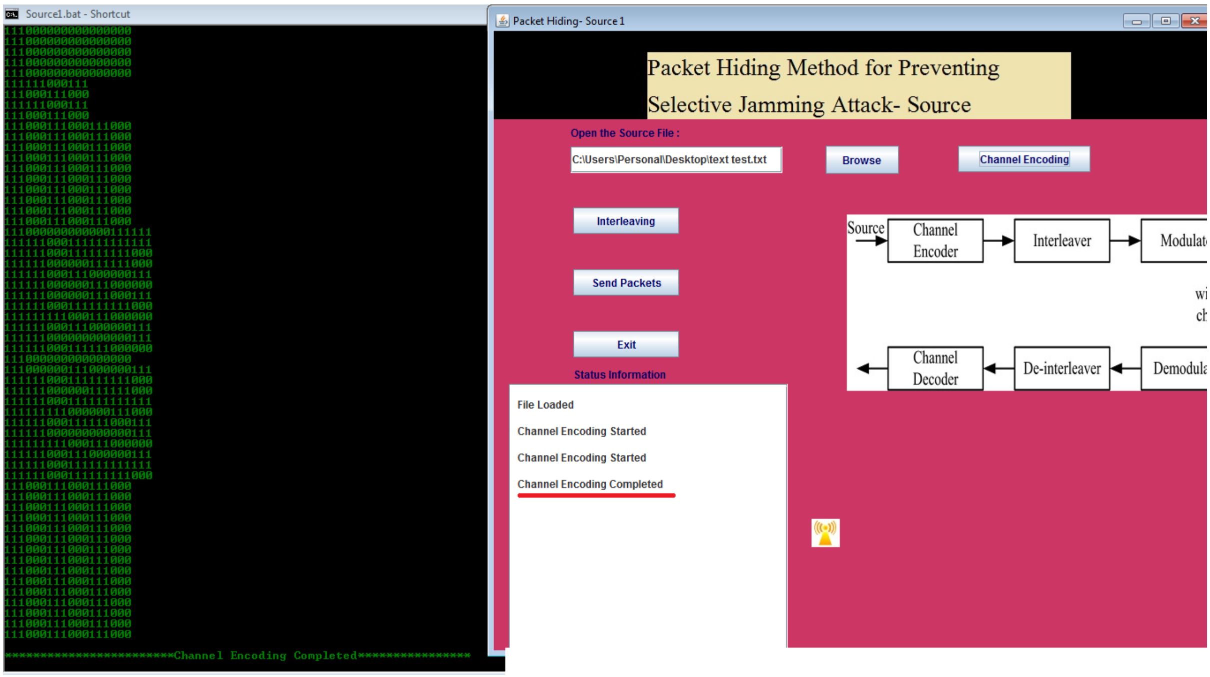
We have built an easy interface to initialize the system rather than giving command prompt Window. It is a simple interface with button built with Java GUI. Three systems are available in this system. An original data file is sent from source to destination with required processes. JDK 1.6 running in Windows 7 operating system. The system uses RMI (Remote method interface). Java SWING API is used to build user interface. The RMI technology lets the nodes communicate remotely. Java awt.event.* is used to perform action/event listener. Encoding and interleaving is performed by event listener. There are encoding, interleaving and packet data sent button which is performed according to the function and the reverse process is used in the destination to regain the original data.

4.5 Problem Implementation

To implement this project, analysis of packet hiding method java 1.6 is used as the front end tool, no backend tool is present. All the process are followed while sending data from sender to receiver and the file which is transferred goes through the process or phases as mentioned above. The phases are as follows.

4.5.1 Channel Encoding

The original text will convert into ASCII values. Here Integer.toBinary() is used. The first step of modulation or encrypting is completed. And the figures are given below.



```
111000000000000000
111000000000000000
111000000000000000
111000000000000000
111000000000000000
111111000111
111000111000
111111000111
111000111000
111000111000111000
111000111000111000
111000111000111000
111000111000111000
111000111000111000
111000111000111000
111000111000111000
111000111000111000
111000111000111000
111000111000111000
111000000000000111111
111111000111111111111
111111000111111111000
111111000000111111000
111111000111000000111
111111000000111000000
111111000000111000111
111111000111111111000
111111111000111000000
111111000111000000111
111111000000000000111
111111000111111000000
111000000000000000
111000000111000000111
111111000111111111000
111111000000111111000
111111000111111111111
111111111000000111000
111111000111111000111
111111000000000000111
111111111000111000000
111111000111000000111
111111000111111111111
111111000111111111000
111000111000111000
111000111000111000
111000111000111000
111000111000111000
111000111000111000
111000111000111000
111000111000111000
111000111000111000
111000111000111000
111000111000111000
111000111000111000
111000111000111000
111000111000111000
111000111000111000
111000111000111000

************************Channel Encoding Completed****************
```

Packet Hiding Method for Preventing
Selective Jamming Attack- Source

Open the Source File :

C:\Users\Personal\Desktop\text test.txt

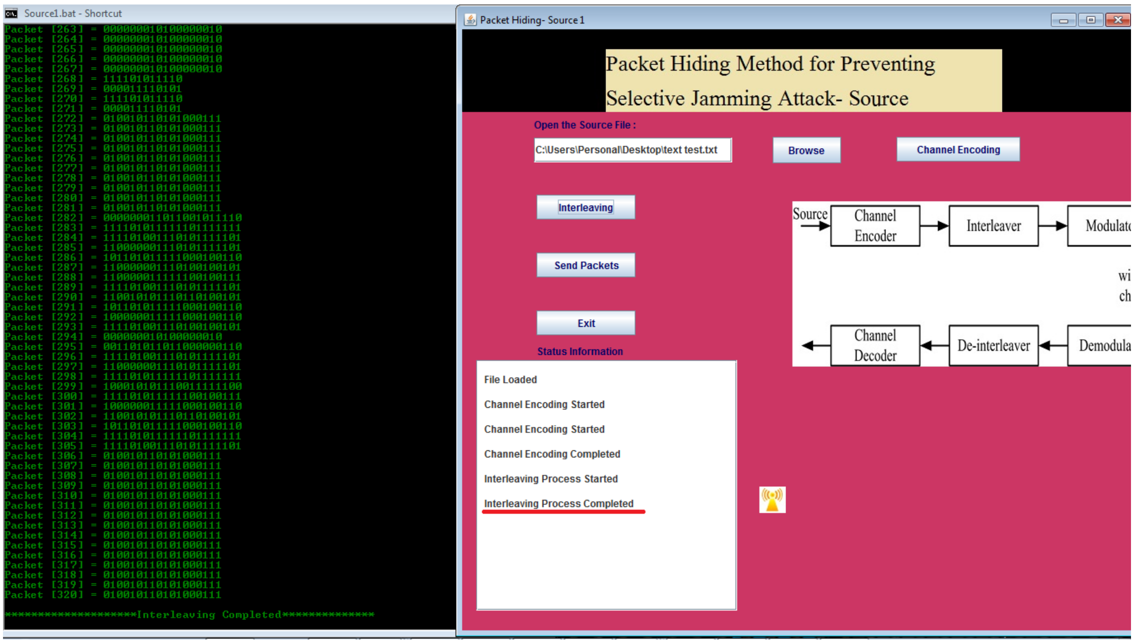
Status Information

File Loaded
Channel Encoding Started
Channel Encoding Started
Channel Encoding Completed

Figure 4.5.1: Channel Encoding

4.5.2 Interleaving

The second step is used to avoid collapses due to burst error. In this step math.random() is used to make simple spacing. This is also the process of sender side.



```
Packet [263] = 0000000101000000010
Packet [264] = 0000000101000000010
Packet [265] = 0000000101000000010
Packet [266] = 0000000101000000010
Packet [267] = 0000000101000000010
Packet [268] = 111101011110
Packet [269] = 000011110101
Packet [270] = 111101011110
Packet [271] = 000011110101
Packet [272] = 0100101101010000111
Packet [273] = 0100101101010000111
Packet [274] = 0100101101010000111
Packet [275] = 0100101101010000111
Packet [276] = 0100101101010000111
Packet [277] = 0100101101010000111
Packet [278] = 0100101101010000111
Packet [279] = 0100101101010000111
Packet [280] = 0100101101010000111
Packet [281] = 0100101101010000111
Packet [282] = 000000011011001011110
Packet [283] = 111101011111101111111
Packet [284] = 111101001110101111101
Packet [285] = 110000001110101111101
Packet [286] = 101101011111000100110
Packet [287] = 110000001110100100101
Packet [288] = 110000011111100100111
Packet [289] = 111101001110101111101
Packet [290] = 110010101110110100101
Packet [291] = 101101011111000100110
Packet [292] = 100000011111000100110
Packet [293] = 111101001110100100101
Packet [294] = 0000000101000000010
Packet [295] = 001101011011000000110
Packet [296] = 111101001110101111101
Packet [297] = 110000001110101111101
Packet [298] = 111101011111101111111
Packet [299] = 100010101110011111100
Packet [300] = 111101011111100100111
Packet [301] = 100000011111000100110
Packet [302] = 110010101110110100101
Packet [303] = 101101011111000100110
Packet [304] = 111101011111101111111
Packet [305] = 111101001110101111101
Packet [306] = 0100101101010000111
Packet [307] = 0100101101010000111
Packet [308] = 0100101101010000111
Packet [309] = 0100101101010000111
Packet [310] = 0100101101010000111
Packet [311] = 0100101101010000111
Packet [312] = 0100101101010000111
Packet [313] = 0100101101010000111
Packet [314] = 0100101101010000111
Packet [315] = 0100101101010000111
Packet [316] = 0100101101010000111
Packet [317] = 0100101101010000111
Packet [318] = 0100101101010000111
Packet [319] = 0100101101010000111
Packet [320] = 0100101101010000111

********************Interleaving Completed**************
```

File Loaded

Channel Encoding Started

Channel Encoding Started

Channel Encoding Completed

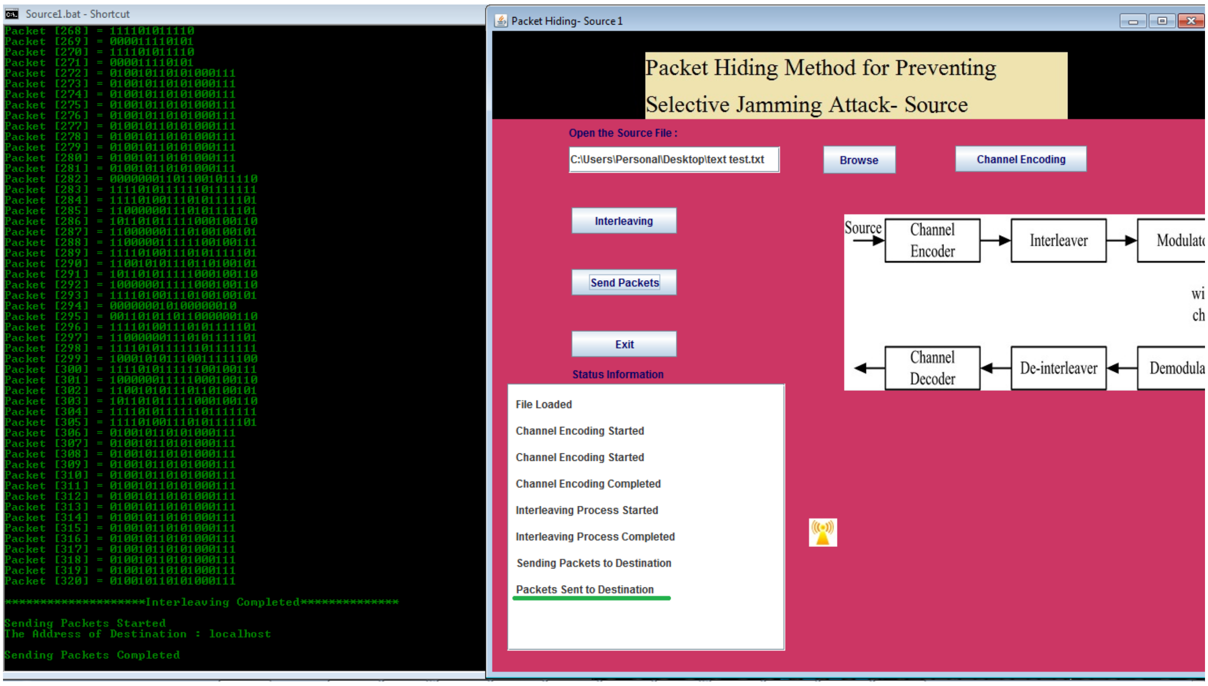
Interleaving Process Started

Interleaving Process Completed

Figure 4.5.2: Interleaving

4.5.3 Modulation

Modulation is the process that modulates the signal into suitable wave from across the communication. Typical modulation techniques are BPSK and QAM. This module can be implemented in the physical level only.



```
Packet [268] = 111101011110
Packet [269] = 000011110101
Packet [270] = 111101011110
Packet [271] = 000011110101
Packet [272] = 0100101101010000111
Packet [273] = 0100101101010000111
Packet [274] = 0100101101010000111
Packet [275] = 0100101101010000111
Packet [276] = 0100101101010000111
Packet [277] = 0100101101010000111
Packet [278] = 0100101101010000111
Packet [279] = 0100101101010000111
Packet [280] = 0100101101010000111
Packet [281] = 0100101101010000111
Packet [282] = 000000011011001011110
Packet [283] = 111101011111101111111
Packet [284] = 111101001110101111101
Packet [285] = 110000001110101111101
Packet [286] = 101101011111000100110
Packet [287] = 110000001110100100101
Packet [288] = 110000011111100100111
Packet [289] = 111101001110101111101
Packet [290] = 110010101110110100101
Packet [291] = 101101011111000100110
Packet [292] = 100000011111000100110
Packet [293] = 111101001110100100101
Packet [294] = 0000000101000000010
Packet [295] = 001101011011000000110
Packet [296] = 111101001110101111101
Packet [297] = 110000001110101111101
Packet [298] = 111101011111101111111
Packet [299] = 100010101110011111100
Packet [300] = 111101011111100100111
Packet [301] = 100000011111000100110
Packet [302] = 110010101110110100101
Packet [303] = 101101011111000100110
Packet [304] = 111101011111101111111
Packet [305] = 111101001110101111101
Packet [306] = 0100101101010000111
Packet [307] = 0100101101010000111
Packet [308] = 0100101101010000111
Packet [309] = 0100101101010000111
Packet [310] = 0100101101010000111
Packet [311] = 0100101101010000111
Packet [312] = 0100101101010000111
Packet [313] = 0100101101010000111
Packet [314] = 0100101101010000111
Packet [315] = 0100101101010000111
Packet [316] = 0100101101010000111
Packet [317] = 0100101101010000111
Packet [318] = 0100101101010000111
Packet [319] = 0100101101010000111
Packet [320] = 0100101101010000111

********************Interleaving Completed**************

Sending Packets Started
The Address of Destination : localhost

Sending Packets Completed
```

File Loaded

Channel Encoding Started

Channel Encoding Started

Channel Encoding Completed

Interleaving Process Started

Interleaving Process Completed

Sending Packets to Destination

Packets Sent to Destination

Figure 4.5.3: Interface of sender server

4.5.4 MAC Layer Format

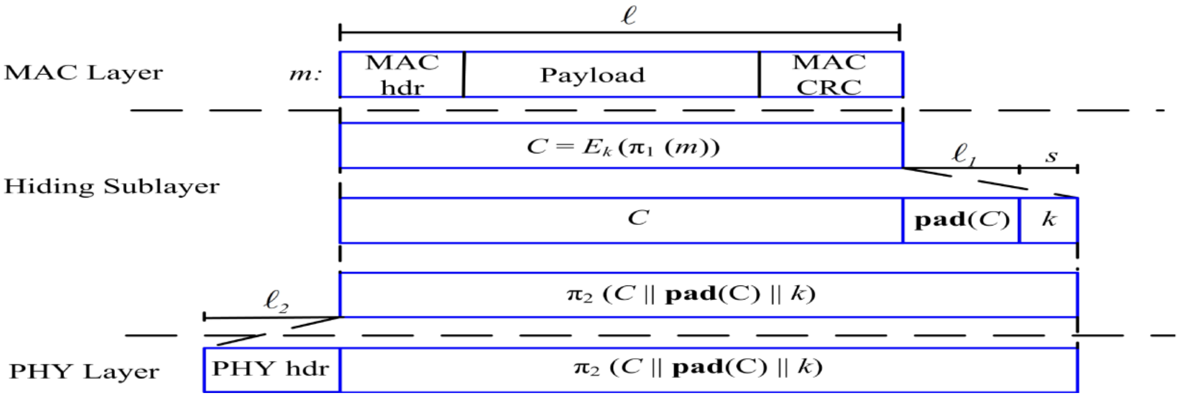


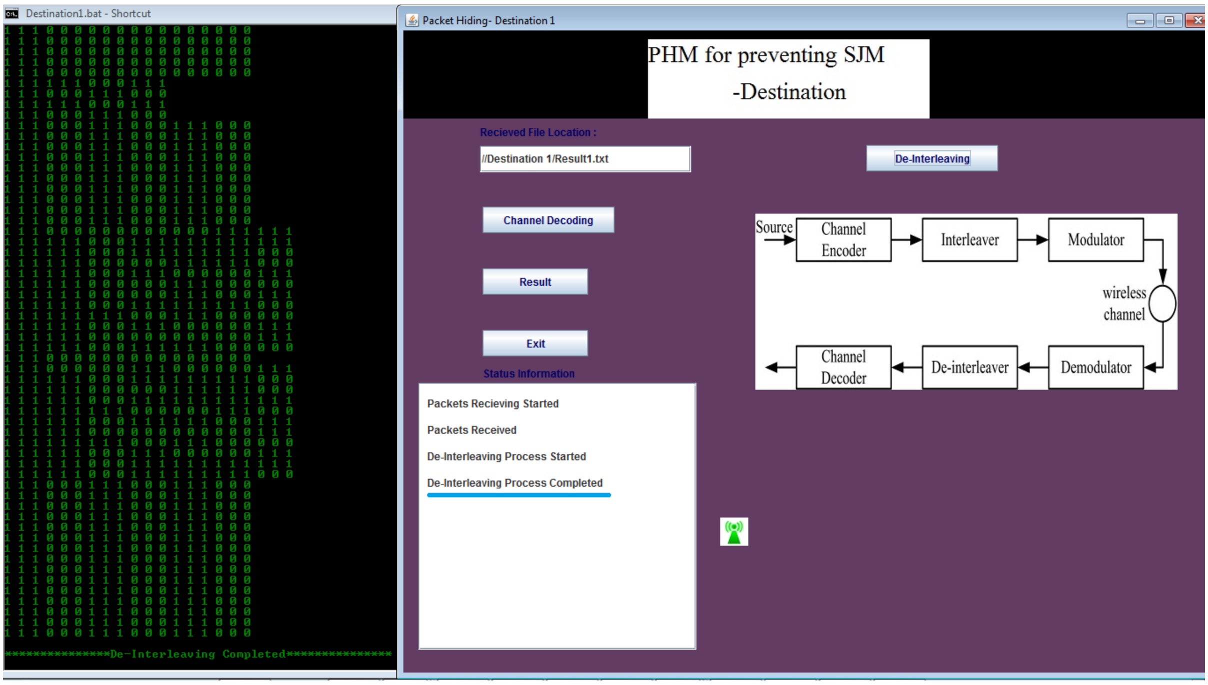
Figure 4.5.4 :MAC layer format

4.5.5 De Modulation

This process is the reverse process of modulation.

4.5.6 De Interleaving

It is the opposite process of interleaving which is used to gain original data. The figures are as follows.



```
1 1 1 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
1 1 1 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
1 1 1 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
1 1 1 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
1 1 1 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
1 1 1 1 1 1 0 0 0 1 1 1
1 1 1 0 0 0 1 1 1 0 0 0
1 1 1 1 1 1 0 0 0 1 1 1
1 1 1 0 0 0 1 1 1 0 0 0
1 1 1 0 0 0 1 1 1 0 0 0 1 1 1 0 0 0
1 1 1 0 0 0 1 1 1 0 0 0 1 1 1 0 0 0
1 1 1 0 0 0 1 1 1 0 0 0 1 1 1 0 0 0
1 1 1 0 0 0 1 1 1 0 0 0 1 1 1 0 0 0
1 1 1 0 0 0 1 1 1 0 0 0 1 1 1 0 0 0
1 1 1 0 0 0 1 1 1 0 0 0 1 1 1 0 0 0
1 1 1 0 0 0 1 1 1 0 0 0 1 1 1 0 0 0
1 1 1 0 0 0 1 1 1 0 0 0 1 1 1 0 0 0
1 1 1 0 0 0 1 1 1 0 0 0 1 1 1 0 0 0
1 1 1 0 0 0 1 1 1 0 0 0 1 1 1 0 0 0
1 1 1 0 0 0 0 0 0 0 0 0 0 0 0 1 1 1 1 1 1
1 1 1 1 1 1 0 0 0 1 1 1 1 1 1 1 1 1 1 1 1
1 1 1 1 1 1 0 0 0 1 1 1 1 1 1 1 1 1 0 0 0
1 1 1 1 1 1 0 0 0 0 0 0 1 1 1 1 1 1 0 0 0
1 1 1 1 1 1 0 0 0 1 1 1 0 0 0 0 0 0 1 1 1
1 1 1 1 1 1 0 0 0 0 0 0 1 1 1 0 0 0 0 0 0
1 1 1 1 1 1 0 0 0 0 0 0 1 1 1 0 0 0 1 1 1
1 1 1 1 1 1 0 0 0 1 1 1 1 1 1 1 1 1 0 0 0
1 1 1 1 1 1 1 1 1 0 0 0 1 1 1 0 0 0 0 0 0
1 1 1 1 1 1 0 0 0 1 1 1 0 0 0 0 0 0 1 1 1
1 1 1 1 1 1 0 0 0 0 0 0 0 0 0 0 0 0 1 1 1
1 1 1 1 1 1 0 0 0 1 1 1 1 1 1 0 0 0 0 0 0
1 1 1 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
1 1 1 0 0 0 0 0 0 1 1 1 0 0 0 0 0 0 1 1 1
1 1 1 1 1 1 0 0 0 1 1 1 1 1 1 1 1 1 0 0 0
1 1 1 1 1 1 0 0 0 0 0 0 1 1 1 1 1 1 0 0 0
1 1 1 1 1 1 0 0 0 1 1 1 1 1 1 1 1 1 1 1 1
1 1 1 1 1 1 1 1 1 0 0 0 0 0 0 1 1 1 0 0 0
1 1 1 1 1 1 0 0 0 1 1 1 1 1 1 0 0 0 1 1 1
1 1 1 1 1 1 0 0 0 0 0 0 0 0 0 0 0 0 1 1 1
1 1 1 1 1 1 1 1 1 0 0 0 1 1 1 0 0 0 0 0 0
1 1 1 1 1 1 0 0 0 1 1 1 0 0 0 0 0 0 1 1 1
1 1 1 1 1 1 0 0 0 1 1 1 1 1 1 1 1 1 1 1 1
1 1 1 1 1 1 0 0 0 1 1 1 1 1 1 1 1 1 0 0 0
1 1 1 0 0 0 1 1 1 0 0 0 1 1 1 0 0 0
1 1 1 0 0 0 1 1 1 0 0 0 1 1 1 0 0 0
1 1 1 0 0 0 1 1 1 0 0 0 1 1 1 0 0 0
1 1 1 0 0 0 1 1 1 0 0 0 1 1 1 0 0 0
1 1 1 0 0 0 1 1 1 0 0 0 1 1 1 0 0 0
1 1 1 0 0 0 1 1 1 0 0 0 1 1 1 0 0 0
1 1 1 0 0 0 1 1 1 0 0 0 1 1 1 0 0 0
1 1 1 0 0 0 1 1 1 0 0 0 1 1 1 0 0 0
1 1 1 0 0 0 1 1 1 0 0 0 1 1 1 0 0 0
1 1 1 0 0 0 1 1 1 0 0 0 1 1 1 0 0 0
1 1 1 0 0 0 1 1 1 0 0 0 1 1 1 0 0 0
1 1 1 0 0 0 1 1 1 0 0 0 1 1 1 0 0 0
1 1 1 0 0 0 1 1 1 0 0 0 1 1 1 0 0 0
1 1 1 0 0 0 1 1 1 0 0 0 1 1 1 0 0 0
1 1 1 0 0 0 1 1 1 0 0 0 1 1 1 0 0 0

***************De-Interleaving Completed***************
```

Recieved File Location : //Destination 1/Result1.txt

Status Information

Packets Recieving Started

Packets Received

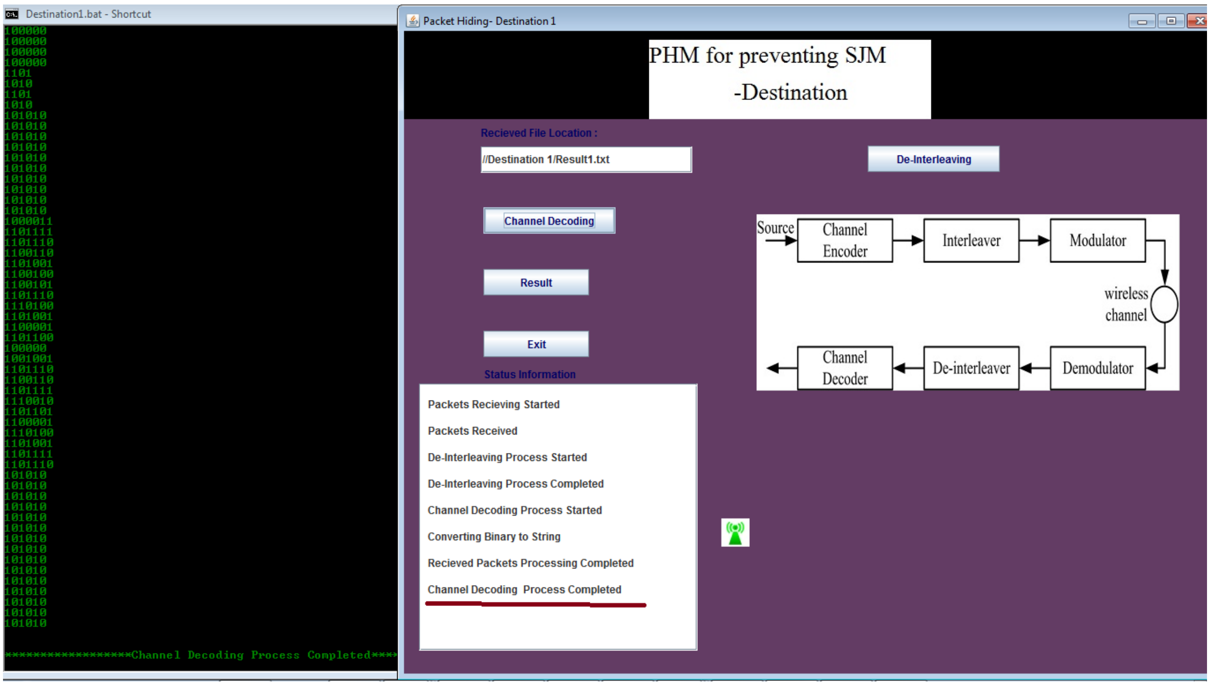
De-Interleaving Process Started

De-Interleaving Process Completed

Figure 4.5.6 :De-interleaving process

4.5.7 Channel Decoding

In this step the ASCII values are converted into original values.



Destination1.bat - Shortcut

```
100000
100000
100000
100000
1101
1010
1101
1010
101010
101010
101010
101010
101010
101010
101010
101010
101010
101010
1000011
1101111
1101110
1100110
1101001
1100100
1100101
1101110
1110100
1101001
1100001
1101100
100000
1001001
1101110
1100110
1101111
1110010
1101101
1100001
1110100
1101001
1101111
1101110
101010
101010
101010
101010
101010
101010
101010
101010
101010
101010
101010
101010
101010
101010
101010


******************Channel Decoding Process Completed****
```

Packet Hiding- Destination 1

PHM for preventing SJM

-Destination

Recieved File Location : //Destination 1/Result1.txt

Status Information

Packets Recieving Started

Packets Received

De-Interleaving Process Started

De-Interleaving Process Completed

Channel Decoding Process Started

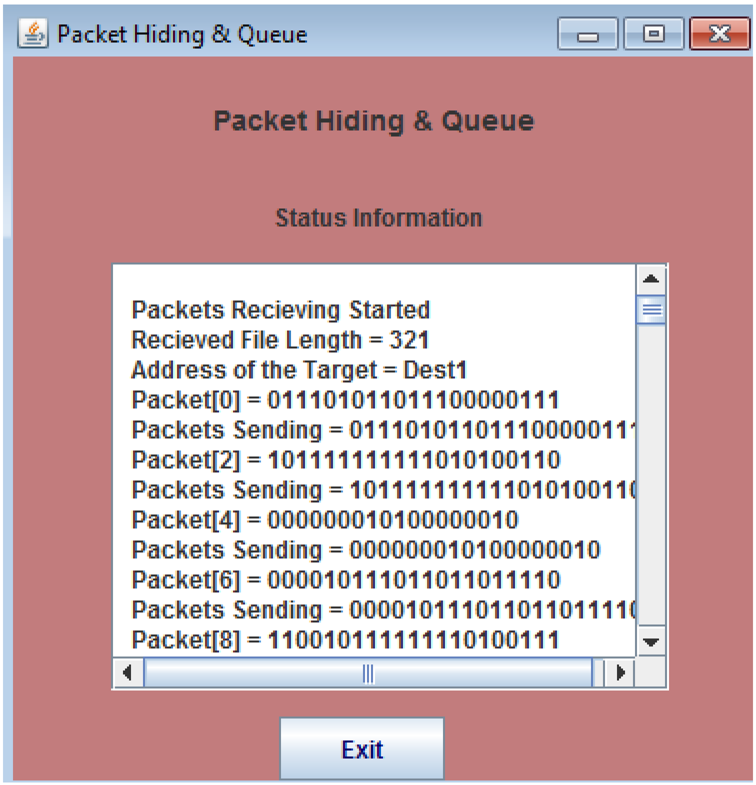
Converting Binary to String

Recieved Packets Processing Completed

Channel Decoding Process Completed

Figure 4.5.7: Channel Decoding

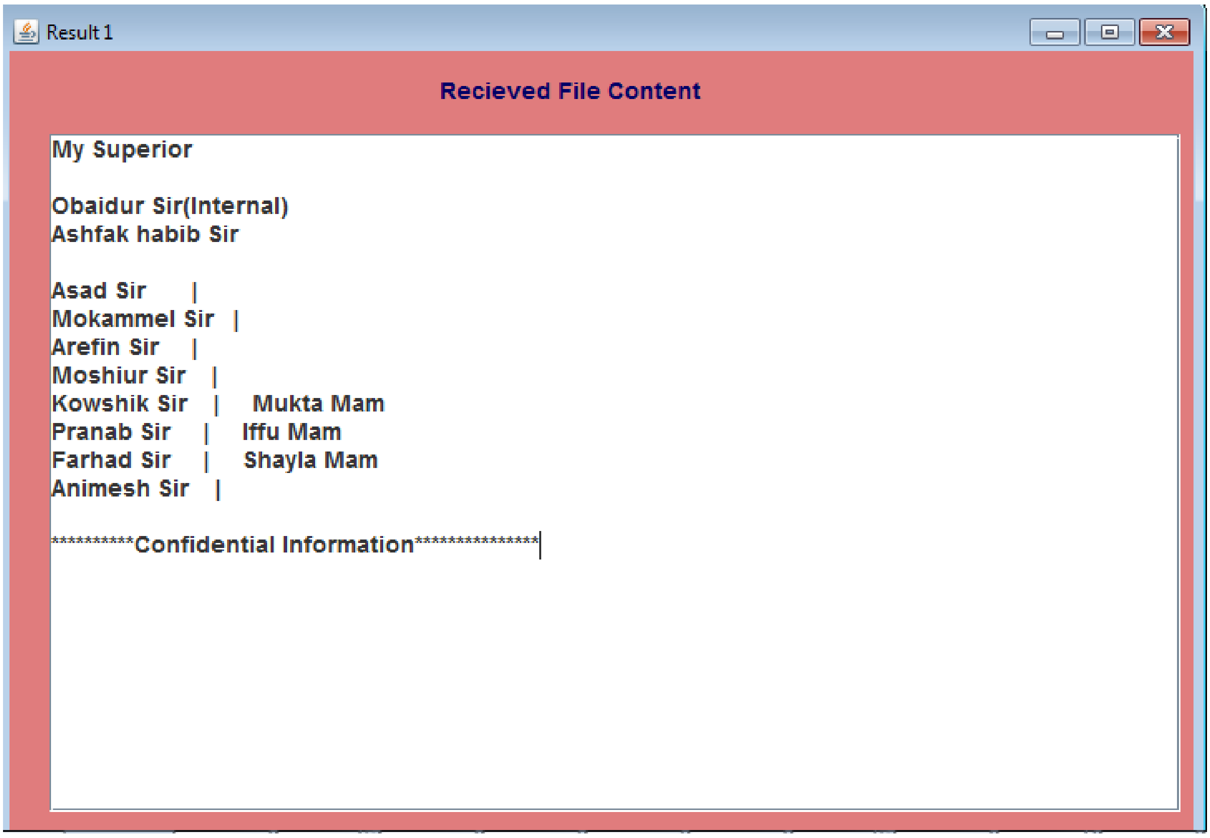
4.5.8 Packet Hiding



```
Packets Recieving Started
Recieved File Length = 321
Address of the Target = Dest1
Packet[0] = 011101011011100000111
Packets Sending = 011101011011100000111
Packet[2] = 101111111111010100110
Packets Sending = 101111111111010100110
Packet[4] = 000000010100000010
Packets Sending = 000000010100000010
Packet[6] = 000010111011011011110
Packets Sending = 000010111011011011110
Packet[8] = 110010111111110100111
```

Figure 4.5.8: Packing Hiding

4.5.9 Destination Server



Recieved File Content

```
My Superior

Obaidur Sir(Internal)
Ashfak habib Sir

Asad Sir      |
Mokammel Sir  |
Arefin Sir    |
Moshiur Sir   |
Kowshik Sir   |    Mukta Mam
Pranab Sir    |    Iffu Mam
Farhad Sir    |    Shayla Mam
Animesh Sir   |

**********Confidential Information**************
```

Figure 4.5.9: Destination Server

4.6 Jamming Attack Analysis

Experiments are made with two clients, two server and a packet hiding queue. The communication flow starts the source sends message to the destination. The message breaks into 48 bytes each and sends them through randomly selected centralized server.

4.6.1 Jamming Attack Geometric Analysis

To analyze the above proposed methodology, let us consider diagrams 1(a) and 1(b). Suppose that AB be the chord of the circle, Point C lies on the circle and Point D lies outside circle.

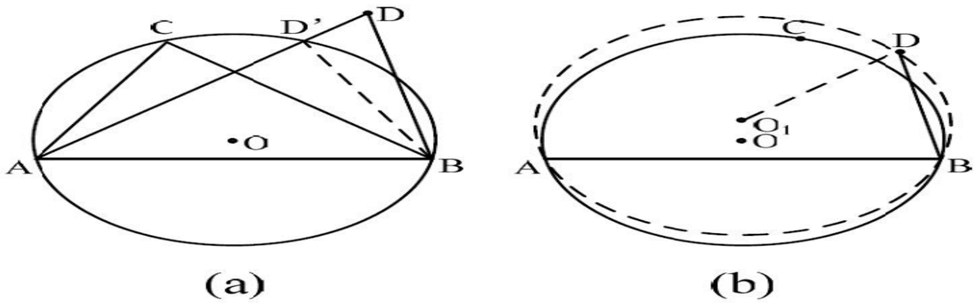


Figure 4.6.1: case 1(a), case 2 (b)

Suppose that the line AD intersects circle at D’. On connecting D’ to B, it can be seen that ∟ACB=∟AD’B. Since ∟ADB=∟ADB+∟D’BD, it proves that ∟ACB >∟ADB.

Next we draw a circum-circle of ΔABD with center as O1. Now is C has to lie within the circle. Because if it lies outside the circle it means that ∟ACB > ∟ADB is proven false, which is a contradiction. Hence jammer position should be the midpoint of the the line joining the nodes separated by maximum distance that covers all the jammed nodes in its circum-circle.

In this project we defined this operation with geometric form where the jamming node can be detected.

4.7 Conclusion

In this chapter we learned about the implementation process and its analysis with respect to geometric analysis. In the next chapter, we can see the detection, prevention and reaction time analysis of the system.

Chapter 5

Experimental Results and Discussion

5.1 Overview

In this chapter we will represent the calculated the performance of our developed system. We have evaluated the system in simulated environment and categorize the evaluation into different parts. As a research based work we point on the quantitative analysis of the evaluation process. We have mainly concentrated on the correctness of the output result. We also analyzed the proper functioning of the system in the practical environment. We considered the accuracy of the result against different acceptance parameter. The experimental result contains input image from physical or simulated environment and generates the corresponding output by comparing the database. For the evaluation of the developed system we performed series of test cases with different criteria. The experiments are elaborated in the later sections.

5.2 Result Analysis for Preventing the Selective Jammer

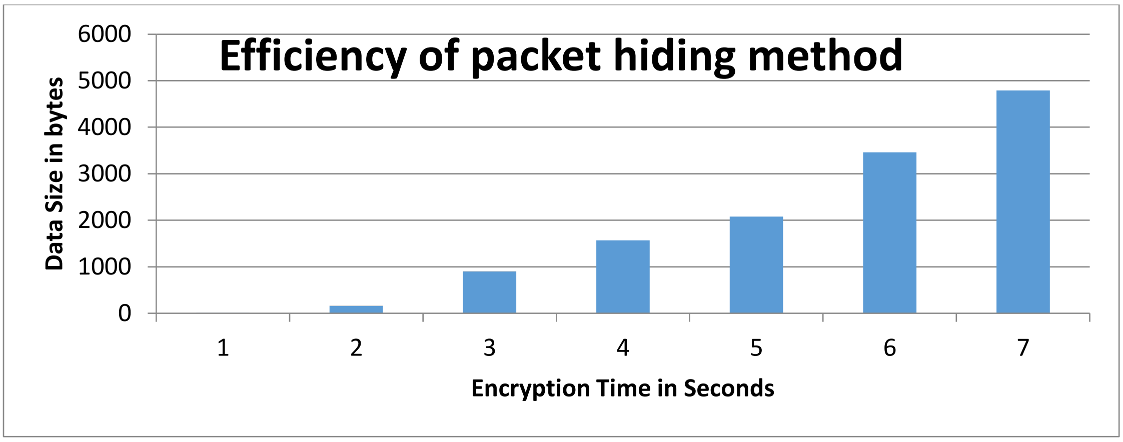


Figure 5.2: Efficiency of packet hiding method

5.3 Comparison with a Different Model

Table 5.3: Comparison of Results

	Average Encryption Time	**Efficiency**
Proposed Model	**15.45s**	**99.52%**
Reference [5]	**20.22s**	**96%**

5.4 Result Analysis for the Detection of Selective Jammer

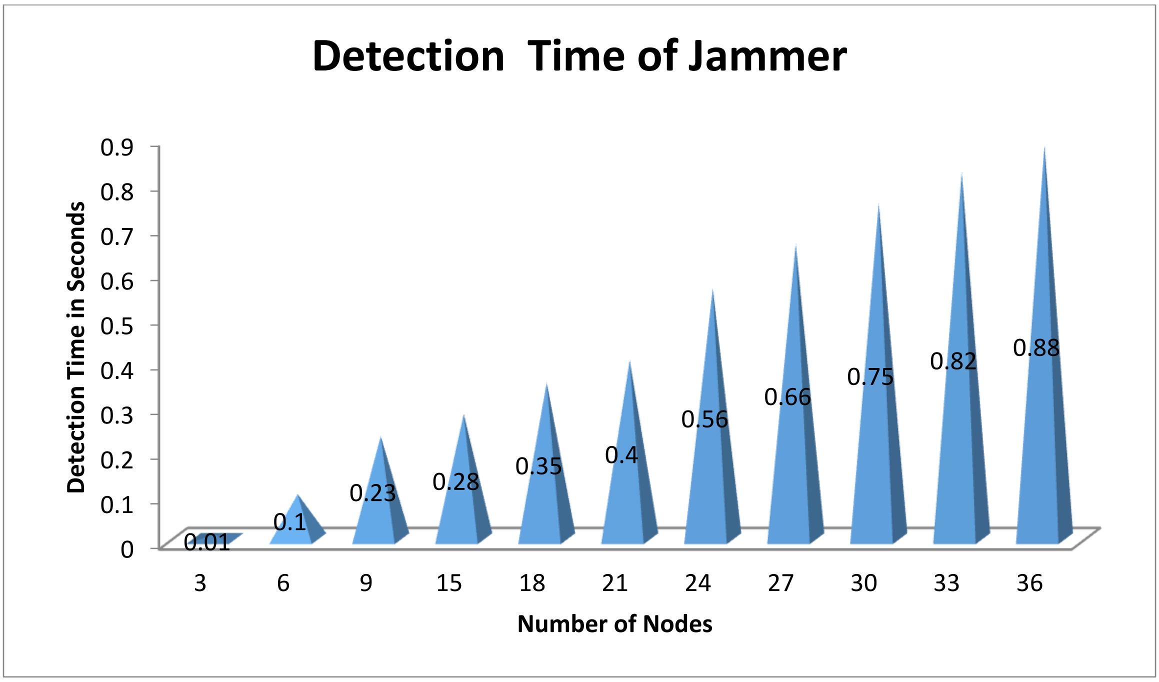


Figure 5.4 : Result Analysis for the Detection of Selective Jammer

5.4.1 Threshold values vs Detection rate

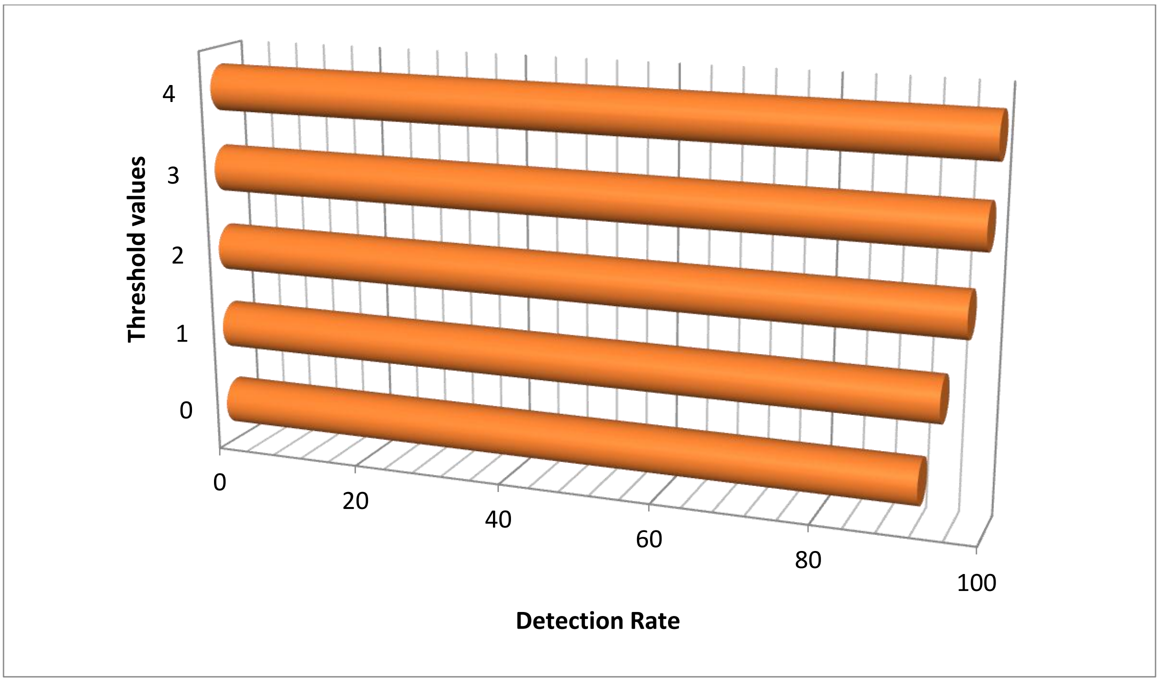


Figure 5.4.1: Chart of Detection Time vs Threshold values

Table 5.4.2 Comparison Between Existing System and Proposed System

Parameter	Existing	Proposed
1.Approach	Decentralized	Centralized
2.Communication During Jamming	Required	Not Required
3.Mapping Process	Crisp logic iteration	Neighborhood check
4.Output	Jamming/no jamming	Exact Jammer Node
5.Average time needed to detect the jammer (50 nodes)	2.75sec	1.67sec
6.Detection	99.23%	99.85%
7.Geometric Explanation	Not given	Given

Chapter 6

Conclusion and Future Recommendation

6.1 Conclusion

In this work entitled on **“Improving Detection, Prevention and Reaction of Selective Jamming Attack Using Packet Hiding Method”** I have analyzed the packet hiding method using Strong Hiding Commitment Scheme and combine with geometrical explanation. Compared to previous work analyzed result it is clear that the combination of SHCS and geometric approach will make the data more secure and fast data transmission.

This project provides solution for jamming attack over wireless network. In this internal threat model jammer is part of the network and has the secret information about the network. The jammer can perform real time classification by decoding first few bytes of transmitted data packet. To prevent real time classification Strong Hiding Commitment Scheme was developed. The jammer can also be located at exact position by geometric approach. I have analyzed the security of our method and quantified their computational and communication overhead.

6.2 Future Recommendations

As further improve of this scheme will compromise support for covering large area. WSN will be commonly used in a near future so it should be tested and implement as perfectly as possible before people use it. In future experiments it would be interesting to analyze other network details and after the implementation of detecting the jammer by advanced technique in future. In our thesis we have implemented a simulation of detection and prevention of selective jamming and showed the geometric approach. It should be examined in real environment. In future, we’ll work on more advanced cryptographic schemes and speed directions of station nodes which will be concerned.

References

[1] T. X. Brown, J. E. James, and A. Sethi, “Jamming and sensing of encrypted wireless ad hoc networks,” *Proceedings of the seventh ACM international symposium on Mobile ad hoc networking and computing - MobiHoc 06*, 2006

[2] M. Cagalj, S. Capkun, and J.-P. Hubaux, “Wormhole-Based Antijamming Techniques in Sensor Networks,” *IEEE Transactions on Mobile Computing*, vol. 6, no. 1, pp. 100–114, 2007.

[3] A. Chan, X. Liu, G. Noubir, and B. Thapa, “Broadcast Control Channel Jamming: Resilience and Identification of Traitors,” *2007 IEEE International Symposium on Information Theory*, 2007.

[4] T. Dempsey, G. Sahin, Y. Morton, and C. Hopper, “Intelligent sensing and classification in ad hoc networks: a case study,” *IEEE Aerospace and Electronic Systems Magazine*, vol. 24, no. 8, pp. 23–30, 2009.

[5] Y. Desmedt, R. Safavi-Naini, H. Wang, L. Batten, C. Charnes, and J. Pieprzyk, “Broadcast anti-jamming systems,” *Computer Networks*, vol. 35, no. 2-3, pp. 223–236, 2001.

[6] K. Gaj and P. Chodowiec, “FPGA and ASIC Implementations of AES,” *Cryptographic Engineering*, pp. 235–294, 2009

[7] O. Goldreich. Foundations of cryptography: *Basic applications. Cam-bridge University Press*, 2004.

[8] B. Greenstein, D. Mccoy, J. Pang, T. Kohno, S. Seshan, and D. Wether-all. Improving wireless privacy with an identifier-free link layer protocol. In Proceedings of MobiSys, 2008.

[9] IEEE. IEEE 802.11 standard. http://standards.ieee.org/getieee802/download/802.11-2007.pdf, 2007.

[10] A. Juels and J. Brainard. Client puzzles: A cryptographic counter-measure against connection depletion attacks. In Proceedings of NDSS,pages 151–165, 1999.

[11] Y. W. Law, M. Palaniswami, L. V. Hoesel, J. Doumen, P. Hartel, and P. Havinga. Energy-efficient link-layer jamming attacks against WSN MAC protocols. ACM Transactions on Sensors Networks, 5(1):1–38, 2009.

[12] L. Lazos, S. Liu, and M. Krunz. Mitigating control-channel jamming attacks in multi-channel ad hoc networks. In Proceedings of the 2nd ACM conference on wireless network security, pages 169–180,2009

[13] Raymond D.R, Midkiff S.F. "Denial of service in wireless networks: Attacks and Defences", IEEE CS Security and Privacy 2008, page 74-81.

[14] A.D.Wood and J.A. Stankovic, "Denial of service in sensor networks," Computer, vol. 35, no. 10, pp. 54-62, oct. 2002.

[15] J. McCune, E.Shi, A.Perrig, and M.K.Reiter, "Detection of Denial-of-message attacks on sensor networks broadcasts", Proc. IEEE symp. Security and Privacy, May 2005.

[16] Mario Cagalj, SrdjanCapkun, Jean-PierroHubau "Wormhole-Based Anti jamming Techniques in sensor networks", IEEE Transactions on mobile computing, vol. 6, no. 1, Jan 2007.

[17] Alejandro Proano and LoukasLazos, "Packet-Hiding methods for preventing Selective Jamming attack", IEEE Transactions on dependable and secure computing, vol. 9, no. 1,Feb-2012. .Akyildiz,W.Su,Y.Sankarasubramaniam, and E.Cayirci, "A Survey on Sensor Networks," IEEE Comm. Magazine, vol. 40, no, 8, 2002.

[18] K. Gaj and P. Chodowiec,"FPGA and ASIC Implementations of AES", Cryptographic Engineering, pp. 235-294 , Springer, 2009.

[19] O. Goldreich, "Foundations of Cryptography: Basic Applications", Cambridge Univ. Press,2004

[20] W.Xu,W.Trappe,Y.Zhang, and T.Wood, "The Feasibility of Launching and Detecting Jamming Attacks in Wireless Networks", proc. MobiHoc '05, pp.46-57, 2005.

[21] B. Schneier, "Applied Cryptography: Protocols, Algorithms, and Source Code in C", 2007

[22] Eugene Y. Vassermann and Nicholas Hopper "Vampire Attacks: Draining Life from Wireless Ad Hoc Sensor Networks" IEEE Trans. Mobile Computing, vol. 12, no. 2, pp. 318-332 Feb-2013

[23] Raymond D. R., Marchany R. C., Brownfield M. I., Midkiff S. F., "Effects of Denial-of Sleep Attacks on Wireless Sensor Network MAC Protocols", IEEE Transactions on Vehicular Technology, Vol. 58, Issue 1, pp. 367-380, January 2009.

[24] Jing Deng, Richard Han, and Shivakant Mishra “Defending against Pathbased DoS Attacks in Wireless Sensor Networks” ACM workshop on security of ad hoc and sensor networks, 2005.

[25] Yih-Chun Hu, Adrian Perrig and David B. Johnson “Packet leashes: A defense against wormhole attacks in wireless ad hoc networks”, INFOCOM, 2003.

[26] Alejandro Proan˜o and Loukas Lazos, “Packet hiding methods for preventing selective jamming attack”, IEEE Transactions on dependable and secure computing, vol. 9, no. 1, january/february 2012.

[27] OPNET^{tm}modeler 14.5. http://www.opnet.com/solutions/network rd/modeler.html.

[28] IEEE 802.11 standard. http://standards.ieee.org/getieee802/download/802.11-2007.pdf, 2007.

Elaboration

AONT = All-or-nothing transform

AODV = Ad hoc On-Demand Distance Vector

BN = Border Node

c = Cipher Text

CPHS = Cryptographic Puzzle Hiding Scheme

DSP = Dummy Significant Packet

E_k = Encryption Key

FN = Free Node

HN = Hopping Node

MD5 = The MD5 algorithm is a widely used hash function producing a 128-bit hash value. Although MD5 was initially designed to be used as a cryptographic hash function, it has been found to suffer from extensive vulnerabilities.

MAC = Media Access Control

PHY = Physical Layer

P = Packet

RN = Receiver Node

RP = Receiver Packet

Rm = Range in meter

SJ = Selective Jamming

SP = Sender Packet

TCP = Transmission Control Protocol