RESEARCH ARTICLE OPEN ACCESS

Legitimate Traffic Jamming Prevention

Ashish. L[1], Naresh Kumar. S[2]
[1]*(M.Tech In Cse Dept, Sr Engineering College Warangal, Andhra Pradesh, India)*
[2]*(Assistant Professor In Cse Dept, Sr Engineering Collegewarangal, Andhra Pradesh, India*)

Abstract
Jamming is one of many exploits used compromise the wireless environment. It works by denying service to authorized users as legitimate traffic is jammed by the overwhelming frequencies of illegitimate traffic. A knowledgeable attacker with the right tools can easily jam the 2.4 GHz frequency in a way that drops the signal to a level where the wireless networks can no longer function. The complexity of jamming is the fact that it may not be caused intentionally, as other forms of wireless technology are relying on the 2.4 GHz frequency as well.
To minimize the impact of an unintentional disruption, it is important to identify its presence. Jamming makes itself known at the physical layer of the network, more commonly known as the MAC (Media Access Control) layer. The increased noise floor results in a faltered noise-to-signal ratio, which will be indicated at the client. It may also be measurable from the access point where network management features should able to effectively report noise floor levels that exceed a predetermined threshold. From there the access points must be dynamically reconfigured to transmit channel in reaction to the disruption as identified by changes at the physical layer. For example, if the attack occurred on an RF corresponding to channel 1, the access point should switch to channel 6 or 11 in order to avoid the attack. However, selecting a different channel does not always eliminate the issue of interference. An experienced attacker will often use all available channels in the attack. When this happens, your only option may be to physically hunt down the attacker and confront them face to face.

I. INTRODUCTION

A packet is the unit of data that is routed between an origin and a destination on the Internet or any other packet-switched network. When any file (e-mail message, HTML file, Graphics Interchange Format file, Uniform Resource Locator request, and so forth) is sent from one place to another on the Internet, the Transmission Control Protocol (TCP) layer of TCP/IP divides the file into "chunks" of an efficient size for routing. Each of these packets is separately numbered and includes the Internet address of the destination. The individual packets for a given file may travel different routes through the Internet. When they have all arrived, they are reassembled into the original file (by the TCP layer at the receiving end).

A packet-switching scheme is an efficient way to handle transmissions on a connectionless network such as the Internet. An alternative scheme, circuit-switched, is used for networks allocated for voice connections. In circuit-switching, lines in the network are shared among many users as with packet-switching, but each connection requires the dedication of a particular path for the duration of the connection.

Interference (Jamming) in wireless networks is an important example of malicious attacks in wireless networks. It is achieved by deliberate transmission of radio signals to disrupt the communication in a wireless network by decreasing the signal-to-interference-noise ratio (SINR). Jamming leads to corrupted packets at the receiver, which results in a lowered throughput.

The jamming model is designed to minimize its dependency on the physical (PHY) layer of the wireless protocol. It consists of the following components:

Jamming intelligence (jammer).This base class provides interfaces to wireless module utility. Detailed jamming strategies such as constant jammer, reactive jammer etc. are implemented in child classes. This class depends on the wireless module utility class.
Jamming detection/ mitigation intelligence (mitigation).

This base class provides interfaces to wireless module utility. Detailed jamming detection/mitigation strategies such as mitigate by channel hop, are implemented in child classes. This class depends on the wireless module utility class.
Wireless module utility (utility).

This class provides a set of functions for jammer and jamming mitigation classes to utilize for implementing their strategies. This class acts as a bridge between the intelligence layer and the PHY layer, separating the intelligence from PHY layer details.
PHY layer driver (driver).
Modification to PHY layer classes are required to provide interface to the utility. The modifications are specific to the PHY layer class one wants to study. Driver also notifies the Energy model, if installed.

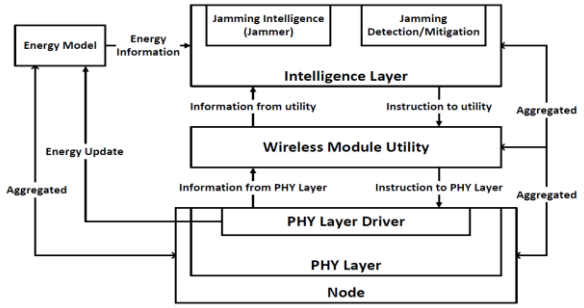


Fig 1 Jamming Hierarchy

1.1. Our Contributions

We investigate the feasibility of real-time packet classification for launching selective jamming attacks. We consider a sophisticated adversary who exploits his knowledge on network protocols along with secrets extracted from compromised nodes to maximize the impact of his attack. To mitigate selective jamming, we combine cryptographic mechanisms such as commitment schemes [6], cryptographic puzzles [7], and all in- one transformation [13], with physical-layer parameters.

We further study the impact of various selective jamming strategies on the performance of the TCP protocol. The remainder of the paper is organized as follows. Section II, presents related work. In Section III, we describe the problem addressed, and state the system and adversarial model assumptions. In Section IV, we illustrate the feasibility of selective jamming attacks. In Section V, we develop methods for preventing selective jamming. Section VI, illustrates the impact of selective jamming on the performance of TCP. In Section VII, we conclude.

II. RELATED WORK

The following types of jammers are categorized by the jamming model:

Eavesdropper jammer: Listens and records wireless traffic in channel(s).

Constant jammer: Sends jamming signal of certain duration at a constant interval.

Random jammer: Sends jamming signal of certain duration at a randomly chosen interval.

Reactive jammer: Sends jamming signal of certain duration only when communication is present in the channel.

Users can easily define their own jamming strategies (classes) following the format in provided classes. The jamming intelligence class is designed to abstract the detail of sending jamming signals and extracting information from the channel.

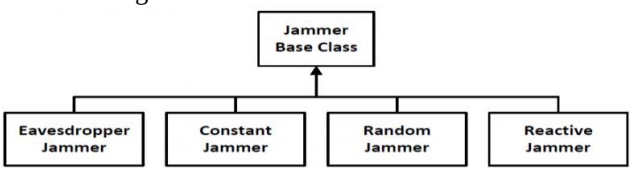


Fig 2 Jammer Structure,

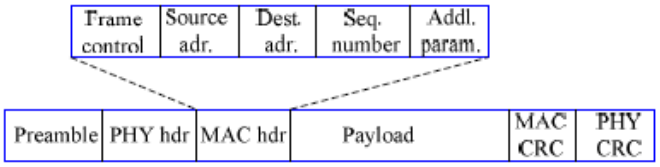


Fig 3 a generic frame format for a wireless network.

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

III. PROPOSED WORK

Here the contribution towards jamming attacks is reduced by using the two algorithms.

3.1. Symmetric encryption algorithm

Symmetric-key algorithms are a class of algorithms for cryptography that use the same cryptographic keys for both encryption of plaintext and decryption of cipher text. The keys may be identical or there may be a simple transformation to go between the two keys. The keys, in practice, represent a shared secret between two or more parties that can be used to maintain a private information link. This requirement that both parties have access to the secret key is one of the main drawbacks of symmetric key encryption, in comparison to public-key encryption. This is also known as private key encryption.

3.2. Brute force attacks against block encryption algorithms

In cryptography, a brute-force attack, or exhaustive key search, is a cryptanalytic attack that can, in theory, be used against any encrypted data (except for data encrypted in an information-theoretically secure manner).

Such an attack might be utilized when it is not possible to take advantage of other weaknesses in an encryption system (if any exist) that would make the task easier. It consists of systematically checking all possible keys or passwords until the correct one is found. In the worst case, this would involve traversing the entire search space.

When password guessing, this method is very fast when used to check all short passwords, but for longer passwords other methods such as the dictionary

attack are used because of the time a brute-force search takes.

When key guessing, the key length used in the cipher determines the practical feasibility of performing a brute-force attack, with longer keys exponentially more difficult to crack than shorter ones. A cipher with a key length of *N* bits can be broken in a worst-case time proportional to $2^N$and an average time of half that.

Brute-force attacks can be made less effective by obfuscating the data to be encoded, something that makes it more difficult for an attacker to recognize when he/she has cracked the code. One of the measures of the strength of an encryption system is how long it would theoretically take an attacker to mount a successful brute-force attack against it.

Brute-force attacks are an application of brute-force search, the general problem-solving technique of enumerating all candidates and checking each one.

The proposed algorithm keeps these two in mind as they are essential in reducing the jamming attacks by using the packet hiding mechanism.

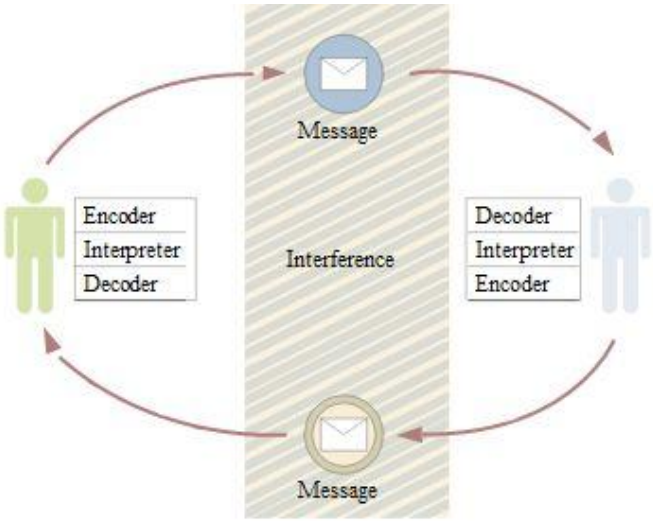
IV. PROBLEM STATEMENT AND ASSUMPTIONS

a. Problem Statement

Consider the scenario depicted in Fig. 1(a). Nodes A and B communicate via a wireless link. Within the communication range of both A and B there is a jamming node J. When A transmits a packet m to B, node J classifies m by receiving only the first few bytes of m. J then corrupts m beyond recovery by interfering with its reception at B. We address the problem of preventing the jamming node from classifying m in real time, thus mitigating J's ability to perform selective jamming. Our goal is to transform a selective jammer to a random one. Note that in the present work, we do not address packet classification methods based on protocol semantics, as described in [1], [4], [11], [33].

b. System and Adversary Model

The network model is a database model conceived as a flexible way of representing objects and their relationships. Its distinguishing feature is that the schema, viewed as a graph in which object types are nodes and relationship types are arcs, is not restricted to being a hierarchy or lattice.



Packets are transmitted at a rate of R bauds. Each PHY-layer symbol corresponds to q bits, where the value of q is defined by the underlying digital modulation scheme. Every symbol carries _ _ q data bits, where α/β is the rate of the PHY-layer encoder. Here, the transmission bit rate is equal to qR bps and the information bit rate is _ _ qR bps.

Communication stands so deeply rooted in human behaviors and the structures of society that scholars have difficulty thinking of it while excluding social or behavioral events. Because communication theory remains a relatively young field of inquiry and integrates itself with other disciplines such as philosophy, psychology, and sociology, one probably cannot yet expect a consensus conceptualization of communication across disciplines

- *Noise*; interference with effective transmission and reception of a message.
- *Sender*; the initiator and encoder of a message
- *Receiver*; the one that receives the message (the listener) and the decoder of a message
- *Decode*; translates the senders spoken idea/message into something the receiver understands by using their knowledge of language from personal experience.
- *Encode*; puts the idea into spoken language while putting their own meaning into the word/message.
- *Channel*; the medium through which the message travels such as through oral communication (radio, television, phone, in person) or written communication (letters, email, text messages)

Feedback; the receivers verbal and nonverbal responses to a message such as a nod for understanding (nonverbal), a raised eyebrow for being confused (nonverbal), or asking a question to clarify the message (verbal).

- *Message*; the verbal and nonverbal components of language that is sent to the receiver by the sender which conveys an idea.

We assume the adversary is in control of the communication medium and can jam messages at any part of the network of his choosing. The adversary can operate in full-duplex mode, thus being able to receive

and transmit concurrently. This can be achieved, for example, with the use of multiple radios. In addition, the adversary is equipped with directional antennas that enable the reception of a signal from one node and jamming of the same signal at another. The adversary is assumed to be computationally bounded, although he can be significantly more powerful than the network devices. Solving well-known hard cryptographic problems is assumed to be time-consuming.

The implementation details of the network functions at every layer of the protocol stack are assumed to be public. For example, the adversary is aware of the digital modulation scheme, the error correction and detection schemes, the MAC, and routing protocol specifications, etc. Furthermore, the adversary is capable of physically compromising network devices and recovering stored information including cryptographic keys, pseudo-random (PRN) sequences, certificates, etc. Hence, the adversary can decrypt any information encrypted with globally known keys, or jam communications protected by globally known PRN sequences.

V. IMPLEMENTATION

The implementation environment has software such as JDK 1.6 running in Windows XP operating system. The system uses Java technology such as RMI (Remote Method Invocation). Java's SWING API is used to build user interface. The RMI technology lets nodes to communicate remotely. The simulation has three kinds of nodes namely centralized server, server and client.

The purpose of source is to send the data to the destination. There sender will be consisting of the Channel Encoder, Interleaver and the Modulator. For simulation of communication in WSN, the server node is able to send messages to client nodes based on the port number and the communication is routed through one of the centralized servers. Here user is able to select a file by clicking browse button. The Send button is to be initiated by user in order to send messages to client based on port number. The message or file selected is broken into packets with length 48 bytes.

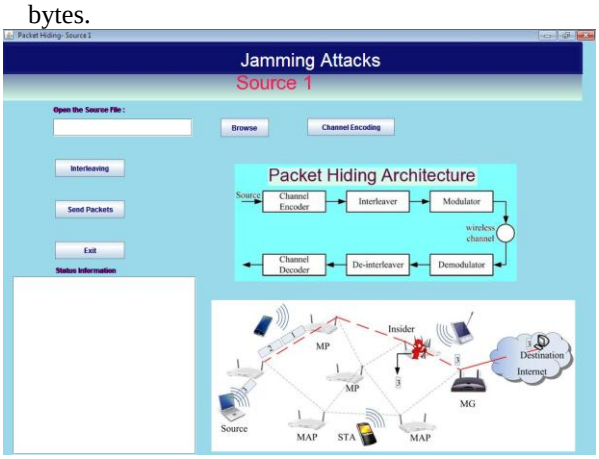


Fig.4 screen shot for source

It selects the required data and sends it to a particular client. The data is sent in the form of packets with length 48 bytes. The server has to use specific IP address and port number based on the centralized server through which it is to send the messages to client. Select the data to transfer by clicking the browse.

Fig .5 File loading

After selecting the file click on the channel encoder. Channel encoding deals with error control during the transmission through the communication channel. It transforms the information sequence to the encoded sequence. The result we get after the modulation is "Code Word". Code word is an element of a standardized code or protocol. Each code word is assembled in accordance with the specific rules of the code and assigned a unique meaning. Code words are typically used for reasons of reliability, clarity, brevity, or secrecy.

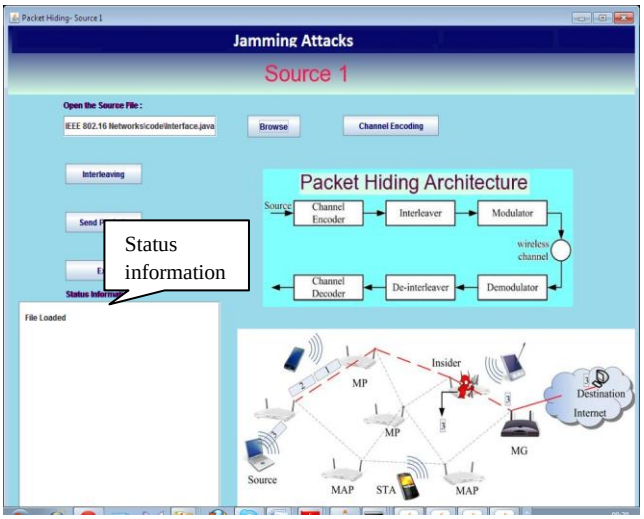


Fig.6 Acknowledgment for loading File

The purpose of channel coding theory is to find codes which transmit quickly, contain many valid code words and can correct or at least detect many errors. While not mutually exclusive,

performance in these areas is a trade off. So, different codes are optimal for different applications. The channel encoding will be done in this way. After the encoding is completed there will be a message displayed.

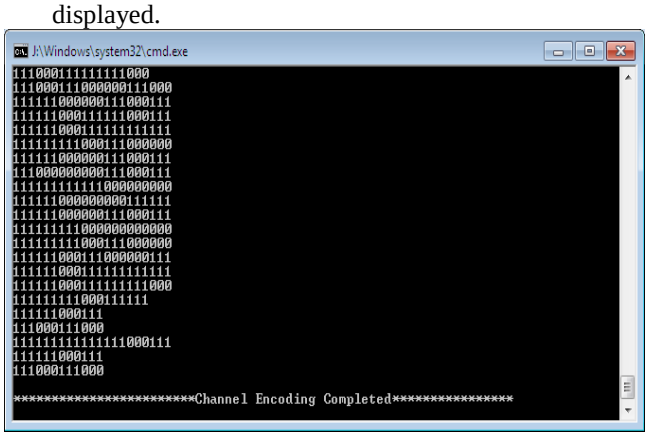


Fig.7 Channel encoding of the data

Interleaving, a technique for making forward error correction more robust with respect to burst errors. Interleaving is a way to arrange data in a non-contiguous way to increase performance. In error-correction coding, particularly within data transmission, disk storage, and memory. After the interleaving the data is converted into packets. Then the packets are used for the transmission. Interleaving the bits of the binary representation of coordinate values to produce a Z-order (curve) for points.

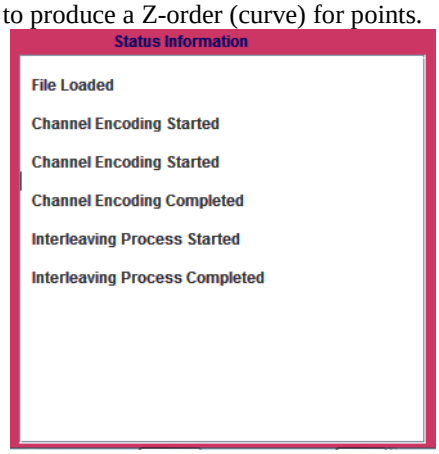


Fig.8 Status Corresponding to particular action

Identify the destination and data is converted into the packets and send to selected destination. If the data is sent properly there will be a message in the "status information"

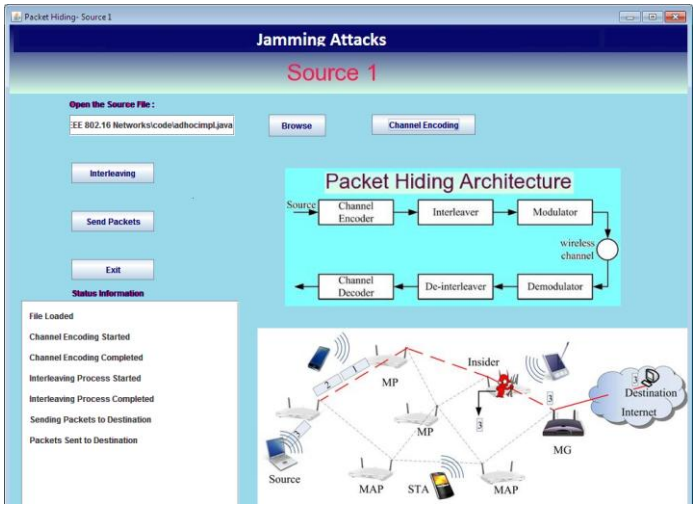


Fig.9 Packet Transmission to the Packet hiding queue

5.1. Packet Hiding

Packet hiding Queue is responsible for sending the packets in a queue format i.e., first come first served the packets which come first will be sent first in a sequential order. The packet hiding acts as a server which is used for identifying the destination. It also checks the size of the data when we are transmitting. Each packet will be storing its corresponding information in the binary format. The packet hiding queue is responsible for sending the data to the destination.

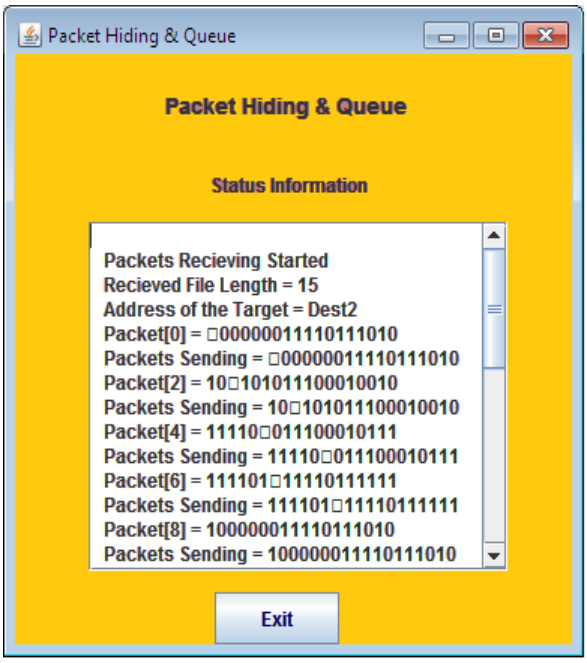


Fig.10 Packet Hiding Queue

When the packet hiding queue sends the data received from the source to the destination. The destination will be ready to take the data from the packet hiding queue.

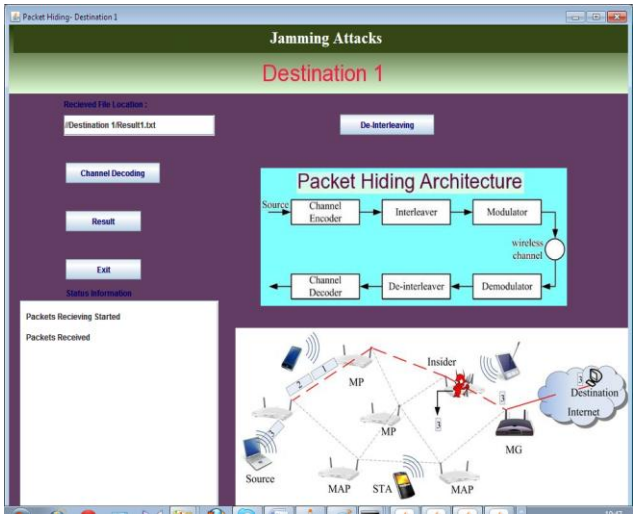


Fig.11 Packets Received at Destination

The destination will be receiving the path from where it can get the data from the packet hiding queue. The Destination will be consisting of the Demodulator, De-interleaver and Channel Decoder.

Demodulation is a process used in the receivers to recover the original signal coming from the sender end in modulating form. At the receiver end, the interleaved data is arranged back into the original sequence by the de-interleaver. As a result of interleaving, correlated noise introduced in the transmission channel appears to be statistically independent at the receiver and thus allows better error correction.

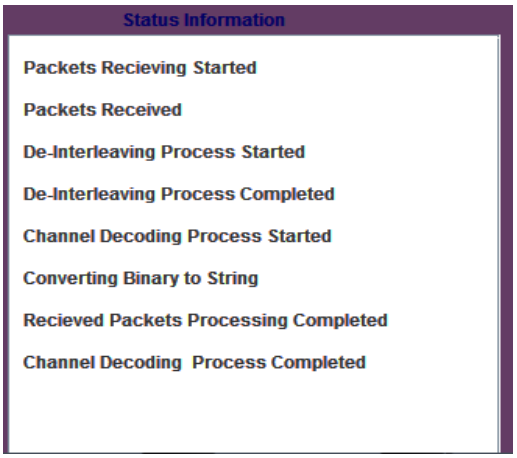


Fig. 12 Status After demodulation, deinterleaving and channel decoding

5.2. File data at the Source

The data sent from the sender is a text file which is consisting the following information.

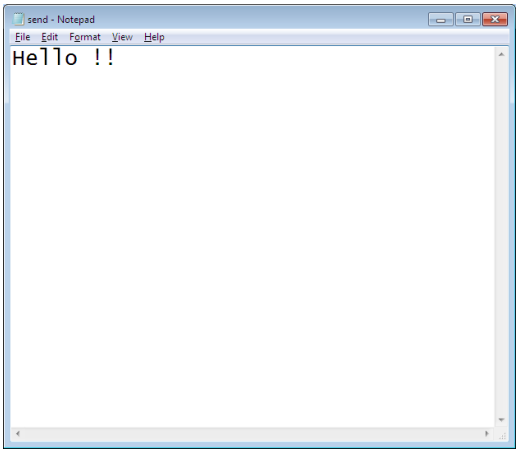


Fig 13 Choose file with the data at Source

5.3. Destination

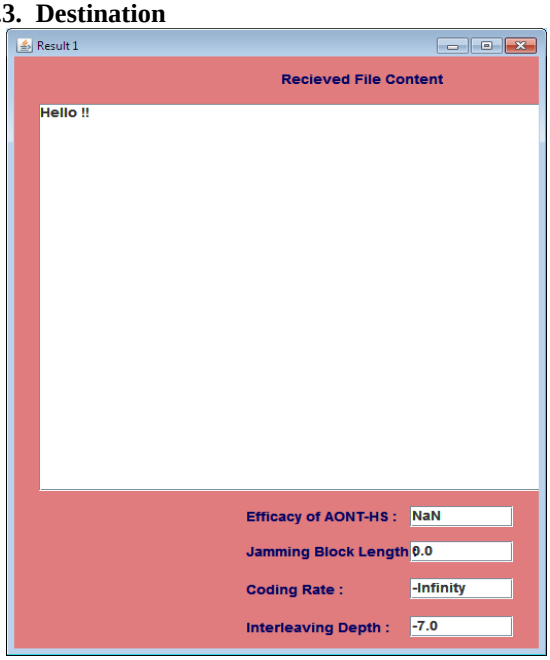


Fig.14 Received data At the destination

The status information text area is meant for presenting status messages.

5.4. The Jamming Attack Analysis

Experiments are made with two clients, two servers and a packet hiding Queue. The communication flow starts when source decides to send messages to client. It chooses a file and breaks it into many packets of size 48 bytes each and sends them through randomly selected centralized server. The server monitors communication and detects any jamming attacks. The jamming Attacks can be viewed by "Jamming Attack Analysis"

When data is sent from source to destination by using the packet hiding queue. It can analyze the attacks and also find whether the attack is made or not. It considers packet loss as well. It is assumed that due to attack in sending packets may occur and in turn it results in data loss or packet loss.

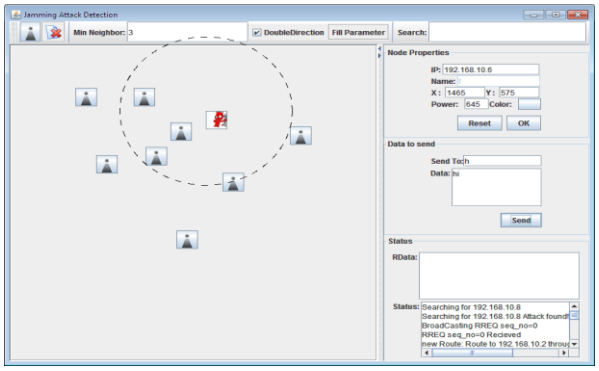


Fig.15 Jamming Attack Detection

As seen in fig, the when the jamming attack is detected then it will be indicated with the red symbol at the corresponding node

I. CONCLUSION

We studied various protocol aware jamming attacks that can be launched in an access point based 802.11b network.

We started by presenting the various jamming attacks ranging from trivial jamming to intelligent jamming attacks such as CTS corrupt jamming. We then presented simulation results showing the effect of misbehaving nodes that do not adhere to the underlying MAC protocol. The network throughput suffered drastically even in the presence of a single misbehaving node and more so with two misbehaving nodes.

We then presented several hybrid attacks that increase the effectiveness of the attack or the decrease the probability of detection of the attack.

REFERENCES

[1] Acharya, M., T. Sharma, D. Thuente, D. Sizemore, *"Intelligent Jammingin 802.11b Wireless Networks", OPNETWORK 2004*, August 2004.

[2] Acharya, M., and D. Thuente, "*Intelligent Jamming Attacks, Counterattacks and (Counter)2 Attacks in 802.11b Wireless Networks", OPNETWORK 2005,* September 2005.

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

[4] Fluhrer, S., I. Martin, I., A. Shamir, "*Weakness in the key scheduling Algorithm of RC4", LNCS, 2259,* 2001.

[5] Kyasanur, P., N. Vaidya, "*Detection and Handling of MAC Layer Misbehavior in Wireless Networks",* DSN 2003.

[6] Leon-Garcia, A., I. Widjaja, "*Communication Networks," McGraw Hill,Boston,* 2000.

[7] Negi, R., A. Rajeswaran, *"DoS Analysis of Reservation Based MAC Protocols*", ICC 2005.

[8] Schiller, J., *"Mobile Communications", Addison-Wesley Longman Publishing, Boston,* 1999.

[9] Lab for Session 1332: *Planning and Analyzing Wireless LANs, OPNETWORK* 2005.

[10] IEEE Std 802.11b-1999/Cor 1-*2001 Standard for wireless LAN mediumaccess control (*MAC)

L. Ashish received the B.Tech Degree in Computer Science & Engineering from Jayamukhi Institute of Technology and Science, Warangal, A.P, India. Currently doing M.tech in Computer Science & Engineering at SR Engineering College, Warangal, India. Research interests include Networking and Security.

Naresh Kumar Sripada is 10 years experienced Assistant Professor in the department Computer Science & Engineering, SR Engineering College, Warangal, India. Research interested area is Software metrics. Expert in teaching Operating Systems and security issues