Enhanced Packet Delivery Techniques Using Crypto-Logic Riddle on Jamming Attacks for Wireless Communication Medium

O.S.C Kesavulu

Assistant Professor, Department of M.C.A., St.Ann's College of Engineering and Technology, Chirala, Prakasam(dt), Andhra Pradesh, India

B.B.V. Satya Vara Prasad

Associate Professor, Department of M.C.A., St.Ann's College of Engineering and Technology, Chirala, Prakasam(dt), Andhra Pradesh, India

Y. Srinivasa Rao

Assistant Professor, Department of M.C.A., St.Ann's College of Engineering and Technology, Chirala, Prakasam(dt), Andhra Pradesh, India

Abstract - In this paper, we address the problem of jamming under an internal threat model. We discuss about Swift jamming attacks in wireless networks. We present a challenger model for selective jamming attacks, which may give to the high importance for packet Delivery Techniques. in which specific messages of "high importance" are targeted We illustrate the impact of selective jamming on the network performance by illustrating various selective attacks against the TCP protocol. We show that such attacks can be launched by performing real-time packet classification at the physical layer. We examine the combination of cryptographic primitives with physical layer attributes for preventing real-time packet classification and neutralizing the inside knowledge of the attacker. 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. we develop three schemes that prevent real-time packet classification by combining cryptographic primitives with physical-layer attributes. Here we propose the Packet delivery techniques on Jamming Attacks over a wire less medium. In this paper we use hiding mechanisms and cryptographic techniques based on the Riddles.

Key words: Jamming Attacks, Wireless Networks Elements , Crypto –logic Riddles, Enhanced Packet Delivery Techniques, wi-fi, Blue Tooth..

I. WIRELESS SYSTEM CHARACTERIZATION

Wireless networks are computer networks that are not connected by cables of any kind. Wireless System enables wireless connectivity to the Internet via radio waves rather than wires on a person's home computer, laptop, Smartphone or similar mobile device. The use of a wireless network enables enterprises to avoid the costly process of introducing cables into buildings or as a connection between different equipment locations. The bases of wireless systems are radio waves, an implementation that takes place at the physical level of network structure. In the computing world, the term "wireless" can be rather ambiguous, since it may refer to several different wireless technologies. The two most common types of wireless capabilities computers have are Blue tooth and Wi-Fi.

II. WI-FI:

Wi-Fi is the technology used for wireless networking. If your computer has a wireless card, it is most likely Wi-Fi compatible. The wireless card transmits to a wireless router, which is also based on the Wi-Fi standard. Wireless routers are often connected to a network, cable modem, or DSL modem, which provides Internet access to anyone connected to the wireless network.

III.   BLUETOOTH

Bluetooth is a specification (IEEE 802.15.1) for the use of low-power radio communications to link phones, computers and other network devices over short distances without wires. The name Bluetooth is borrowed from Harald Bluetooth, a king in Denmark more than 1,000 years ago. Bluetooth technology was designed primarily to support simple wireless networking of personal consumer devices and peripherals, including cell phones, PDAs, and wireless headsets. Wireless signals transmitted with Bluetooth cover short distances, typically up to 30 feet (10 meters). Bluetooth devices generally communicate at less than 1 Mbps. Bluetooth is the technology often used for wireless keyboards and mice, wireless printing, and wireless cell phone headsets. In order to use a device such as a Bluetooth keyboard or mouse, your computer must be Bluetooth-enabled or have a Bluetooth adapter installed. Computers may also use other wireless technologies aside from Wi-Fi and Bluetooth. Products such as remote controls and wireless mice may use infrared or other proprietary wireless technologies. Because of the many wireless options available, it is a good idea to check the system requirements of any wireless device you are considering buying. Bluetooth networks feature a dynamic topology called a **piconet** or PAN. **Piconets** contain a minimum of two and a maximum of eight Bluetooth peer devices. Devices communicate using protocols that are part of the Bluetooth Specification. Definitions for multiple versions of the Bluetooth specification exist including versions 1.1, 1.2 and 2.0.

IV.   WIRELESS NETWORK ELEMENTS

The telecommunications network at the physical layer also consists of many interconnected wire line Network Elements (NEs). These NEs can be stand-alone systems or products that are either supplied by a single manufacturer, or are assembled by the service provider (user) or system integrator with parts from several different manufacturers.

Wireless NEs are products and devices used by a wireless carrier to provide support for the backhaul network as well as a Mobile Switching Center (MSC).Reliable wireless service depends on the network elements at the physical layer to be protected against all operational environments and applications.

Fig:1 Wireless Access Pint

What are especially important are the NEs that are located on the cell tower to the Base Station (BS) cabinet. The attachment hardware and the positioning of the antenna and associated closures/cables are required to have adequate strength, robustness, corrosion resistance, and rain/solar resistance for expected wind, storm, ice, and other weather conditions. Requirements for individual components, such as hardware, cables, connectors, and closures, shall take into consideration the structure to which they are attached.

Fig 2: Network System of wireless network

cross-layer framework for design of ad-hoc wireless networks to support delay-critical applications, such as conversational voice or real-time video. The framework incorporates adaptation across all layers of the protocol stack to leverage the flexibility offered by joint optimization of design parameters.

In Figure 1 we present a wireless network is a collection of wireless nodes that self organize into a network without the help of an existing infrastructure. Some or possibly all of these nodes are mobile. Since the network can be deployed rapidly and flexibly, it is attractive to numerous potential applications, ranging from multi-hop wireless broadband Internet access to highway automation.

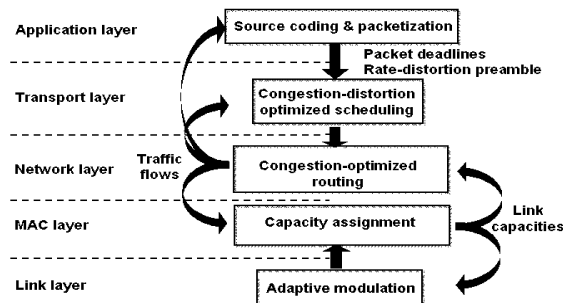## V. LAYER COMMUNICATION SYSTEM OF WIRELESS NETWORKS:

Fig3. Layer Internal Structure

Adaptive link layer techniques will be used to adjust the capacity of individual wireless links to support delay-constrained traffic, possibly in multiple service classes; dynamic capacity assignment in the media access (MAC) layer will optimally allocate resources among various traffic flows; a congestion-optimized routing algorithm will provide multiple paths to real-time media streams; finally at the transport and application level, intelligent packet scheduling and error-resilient audio/video coding will be optimized for low-latency delivery over wireless networks.

VI. PACKET STRUCTURE OF WIRELESS NETWORK:

A packet is one unit of binary data capable of being routed through a computer network. To improve communication performance and reliability, each message sent between two network devices is often subdivided into packets by the underlying hardware and software. Depending on the protocol(s) they need to support, packets are constructed in some standard packet format. Packet formats generally include a header, the body containing the message data (also known as the payload), and sometimes a footer (also known as the trailer).
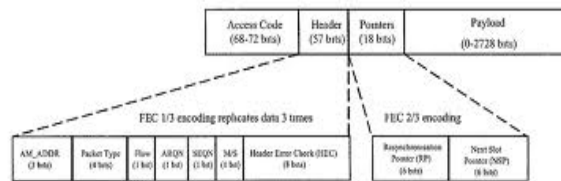
The packet header lists the destination of the packet (in IP packets, the destination IP address) and often indicates the length of the message data. Payload - Also called the body or data of a packet. This is the actual data that the packet is delivering to the destination. If a packet is fixed-length, then the payload may be padded with blank information to make it the right size The packet footer contains data that signifies the end of the packet, such as a special sequence of bits known as a magic number. Both the packet header and footer may contain error-checking information.

The receiving device is responsible for re-assembling individual packets into the original message, by stripping off the headers and footers and concatenating packets in the correct sequence.

VII. WHAT IS JAMMING?

Since RF (radio frequency) is essentially an open medium, jamming can be a huge problem for wireless networks. 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. Some

widely used consumer products include cordless phones, Bluetooth-enabled devices and baby monitors, all capable of disrupting the signal of a wireless network and faltering traffic.

Wireless networks, however adopting the common are as the channel, are more susceptible to be disruptive than those who communicate based on a wire channel such as TP (twist pairs), coaxial cable and fiber. Usually, denial of service aims at filling user-domain and kernel-demain buffers. Because of the shared characteristics, an adversary called Jammer can easily interfere the wireless communication channel using RF technologies either by transmitting a great deal of unmeaning signal disregarding MAC protocols or using valid signal to treat MAC protocols. A variety of jamming attacks can be performed in order to interfere the wireless communication channel. The most efficient attacks can be reduce into four types.

> **Stable Jammer**
> **Misleading Jammer**
> **Random Jammer**
> **Swift Jammer**

Stable Jammer: Continually send random and meaningless signal to the channel disregarding the MAC protocols and Sends jamming signal of certain duration at a constant interval.

Misleading Jammer: Continually injects valid packets which means a valid packet header with a useless payload or even no payload to the channel with no gap between packets.

Random Jammer: Alternate between jamming and sleeping mode. In brief, the jammer perform constant jammer or deceptive jammer for a random period then shut down the jammer for another random period of time. The benefit of this jammer is saving energy which is especially important in a war. Sends jamming signal of certain duration at a randomly chosen interval

Swift Jammer: Stay quiet till there is activity on the channel then devastate the reception. Its target aims at the receiver. Reactive Jammer spent more energy on sensing the channel then corrupted transmitting signal using only a minimum amount of power which brings more imperceptibility. Sends jamming signal of certain duration only when communication is present in the channel.

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

To defend the above from jammers, the first step is to detect the existence of jammer because many other factors can also result in the similar appearance like jammer performed such as low SNR (Signal Noise Ratio), battery running out of power or receiver moving out of the range. A lot of detection methods have been proposed such as Signal Strength detection, Carrier sensing time detection and PDR (Packets Delivery Ratio) detection, however each of which has their own weak point. The current state of art is Signal Strength Consistency Checks which can differentiate jamming from normal signals. However, the only problem of Strength Consistency Checks is it can not differentiate between the various categories of jamming attacks. To enable the network to perform defense strategies more effectively such as saving power or quickly enough reaction, distinguishing the type of different jamming attacks is necessary.
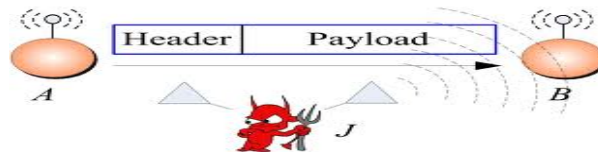

Fig 4. Selective jamming attack

Consider the above Fig 4. 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.

VIII. CONCURRENT PACKET ORGANIZATION

How the adversary can classify packets in real time, before the packet transmission is completed. Once a packet is classified, the adversary may choose to jam it depending on his strategy. Consider the generic communication system depicted in below Figure
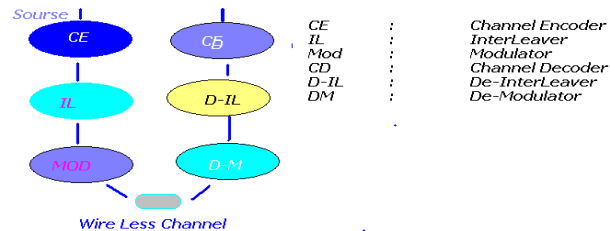

Fig 5. A generic communication system diagram

At the PHY layer, a packet m is encoded, interleaved, and modulated before it is transmitted over the wireless channel. At the receiver, the signal is demodulated, de-interleaved, and decoded, to recover the original packet **m.** The adversary's ability in classifying a packet m depends on the implementation of the blocks in Fig. 2. The channel encoding block expands the original bit sequence m, adding necessary redundancy for protecting m against channel errors.

IX. ENHANCED PACKET DELIVERY TECHNIQUES

In this section, we show that the problem of real-time packet classification can be mapped to the hiding property of binder schemes, and propose a packet-hiding scheme based on binder. In our context, the role of the committer is assumed by the transmitting node S. The role of the verifier is assumed by any receiver R, including the jammer J. The committed value m is the packet that S wants to communicate to R. To transmit m, the sender computes the corresponding binder/de-binder pair (C, d), and broadcasts C. The hiding property ensures that m is not revealed during the transmission of C. To reveal m, the sender releases the de-commitment value d, in which case m is obtained by all receivers, including J. Here We explain in detail about packet delivery Techniques.

Secrete Technique
Here we explain a method Secrete Technique which includes the symmetric cryptography. Encryption is the security solution most applicable in computing. In recent years asymmetric Algorithms have been extensively studied in embedded systems with low computational power. Data encryption emerged before the invention of computer. a cryptographic algorithm can be set as a function that converts encrypted message in clear messages and vice versa, making use of a cryptographic key. Most cryptographic algorithms are public. Secrecy is the key that has the function to parameterize the cryptographic function; i.e only with the key can encrypt or decrypt a message. Another important factor is that the key have the ability to change the output of the algorithm, so every change of key cryptographic algorithm generates a new encrypted message. The key size is critical in a project, because the longer the key, more work will be crypto analyst to try to decipher the message. In general, keys have sizes of 64, 128 or 256 bits and may be higher or lower, according to security needs. Symmetric encryption or secret key cryptography is the use of only a key, both in the encryption and decryption of data. By the year 1976 this was the only known method for the use of encryption, but to be effective you need a secure channel for communication in which a cryptographic key can be changed.

Figure 6

The above figure illustrates a communication through symmetric encryption. The text is encrypted X and Y become the message through the encryption algorithm and key k. The message Y is sent to the receiver, which uses the key k to decrypt it, turning it on again in the text X. Also according to figure 6 you can see that the key k is transported by

a secure channel, for the possession of it, a potential attacker could easily make the reading the original text. AES and DES are two examples of algorithms that are part of the class symmetrical.

Our Main Aim is to satisfy the heavy secrecy on hiding property. Assume   sender S has send the Packet m for R then sender construct the Secrete Technique, its includes the any Encryption Algorithm. Like AES,DES..etc .
$$(C, d) = commit(m),$$
where,
$$C = Ek(\pi 1(m)), d = k.$$

Here, the function Ek() is a symmetric encryption algorithm $\pi 1$ is a publicly known permutation, and $k \in \{0, 1\}s$ is a randomly selected key of some desired key length s (the length of k is a security parameter). The sender broadcasts (C‖d), where "‖" denotes the concatenation operation. Upon reception of d, any receiver R computes

$$m = \pi^{-1}(Dk(C))$$

where $\pi-1$ denotes the inverse permutation of $\pi 1$. To satisfy the 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.

Cryptologic Riddle
In this section, we present a packet beating system based on Cryptologic Riddle. The main idea behind such riddles is to force the recipient of a riddle execute a pre-defined set of calculations before he is able to extract a secret of interest. The advantage of the puzzle based scheme is that its security does not rely on the PHY layer parameters. There are several ways of classifying cryptographic algorithms. They will be categorized based on the number of keys that are employed for encryption and decryption, and further defined by their application and use. The three types of algorithms that will be discussed

- Secret Key Cryptography (SKC): Uses a single key for both encryption and decryption
- Public Key Cryptography (PKC): Uses one key for encryption and another for decryption
- Hash Functions: Uses a mathematical transformation to irreversibly "encrypt" information

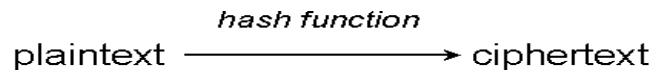Here the technique Croptologic Riddle based on hashing.

Fig 7: Hash Functions

Computationally limited receivers can incur significant delay and energy consumption when dealing with modulo arithmetic. In this case, Cryptologic Riddle can be implemented from cryptographic puzzles which employ computationally efficient cryptographic primitives. Cryptologic Riddle are primitives originally suggested by Merkle as a method for establishing a secret over an insecure channel. They find a wide range of applications from preventing DoS attacks to providing broadcast authentication and key escrow schemes.
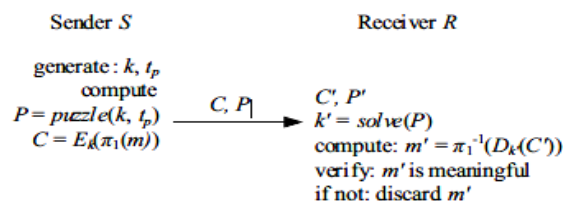

Fig 8. Cryptologic Riddle -based hiding scheme

In our context, we use cryptographic puzzles to temporary hide transmitted packets. A packet m is encrypted with a randomly selected symmetric key k of a desirable length s. The key k is blinded using a cryptographic puzzle and sent to the receiver. For a computationally bounded 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. Let a sender S have a packet m for transmission. The sender selects a random key k ∈ {0, 1}s, of a desired length. S generates a puzzle P = puzzle(k, tp), where puzzle() denotes the puzzle generator function, and tp denotes the time required for the solution of the puzzle. Parameter tp is measured in units of time, and it is directly dependent on the assumed computational capability of the adversary, denoted by N and measured in computational operations per second.

After generating the puzzle P, the sender broadcasts (C, P), where C = Ek(π1(m)). At the receiver side, any receiver R solves the received puzzle P′ to recover key k′ and then computes m′ = π−1(Dk′ (C′)). If the decrypted packet m′ is meaningful (i.e., is in the proper
format, has a valid CRC code, and is within the context
of the receiver's communication), the receiver accepts that m′ = m. Else, the receiver discards m′. Fig. 8 shows the details of Cryptologic Riddle.

Her we discuss about various types of Riddles, which are worked based on the crypotologic.

- **Time-Lock Riddle**
- **Simple Substitution Cipher Riddle**
- **Transposition Ciphers Riddle**
- **Book Cipher Riddle**
- **Poly-Alphabetic Cipher Riddle.**
- **Poly-Graphic Cipher Riddle**

Time-lock Riddles:

Rivest et al. proposed a construction called time-lock puzzles, which is based on the iterative application of a precisely controlled number of modulo operations [22]. Time-lock puzzles have several attractive features such as the fine granularity in controlling tp and the sequential nature of the computation. Moreover, the puzzle generation requires significantly less computation compared to puzzle solving.

In a time-lock puzzle, the puzzle constructor generates
a composite modulus g = u □ v, where u and v are two
large random prime numbers. Then, he picks a random
a, 1 < a < g and hides the encryption key in
Kh = k + a2t mod g, where t = tp □ N, is the amount of time required to solve for k. Here, it is assumed that the solver can perform N squaring modulo g per second. Note that Kh can be computed efficiently if φ(g) = (u − 1)(v − 1) or the factorization of g are known, otherwise a solver would have to perform all t squaring to recover k. The puzzle consists of the values P = (g,Kh, t, a).

Simple Substitution Cipher Riddle:

A substitution cipher is very simple – replace every letter of the alphabet with some other letter or symbol. The key to this cipher is the mapping of one set of letters to another. It Include the following Riddles

Caesar Riddle

The Caesar cipher is named after Julius Caesar, who made use of it to communicate securely with his trusted lieutenants. Caesar used this cipher with an offset (key value) of 3. To encrypt a letter in a message, he would find the 3rd letter in the alphabet after the one he wanted to encrypt. A would become D, B would become E, and so on (and if he went beyond Z, he'd start over again at A).

Fig 9: Cipher Wheel

A cipher wheel is a disc consisting of an inner and outer wheel with the alphabet written around the edge of both wheels. By turning one of the wheels by the offset value, For this reason, the Caesar cipher is often called "ROT" (short for "rotate"), and "ROT" is often followed by the offset amount. So Caesar's cipher would be called "ROT3". The cipher wheel shown below implements ROT7 (going from inside out) or ROT19 (going from outside in). he hint in a cache description page is encrypted using a Caesar cipher with an offset of 13 (aka, ROT13). This value is convenient because the encryption and decryption methods are exactly the same – A encrypts to N, and N encrypts to A.

At bash Riddle

The At bash cipher substitutes each letter of the alphabet with the letter at the opposite end of the alphabet. For instance, A goes to Z, B goes to Y, C goes to X, etc. The name "At bash" comes from its origins in the Hebrew language, where the letter aleph goes to tav, beth goes to shin, etc. The method can be used in any language that has an ordered alphabet.

Cryptogram Riddle

You've probably seen cryptograms in newspapers, near the comics and the crossword Riddle. A cryptogram is a Riddle consisting of a short quotation encrypted using a simple substitution cipher. The mapping from plaintext to cipher text letters is random – there is no ordering to the cipher text letters, like there is in the Caesar and At bash ciphers. The Riddle is to figure out the mapping and reveal the quotation.

Poly-alphabetic Cipher Riddle:

The fundamental problem with all simple substitution ciphers is that they can be attacked using a cryptanalysis method called frequency analysis. This is just a fancy way of saying "count the number of times each letter or symbol appears in the cipher text". The letter that appears the most is probably E, followed closely by T, A, O, I, and N. Complex substitution ciphers were developed to foil attempts to break the code via frequency analysis. The goal of these methods is to try to get all symbols in the cipher text to appear with roughly the same frequency. A poly alphabetic cipher is one in which a single cipher text letter does not correspond to a single plaintext letter. The letter A at one point in the cipher text may decode to a completely different letter than an A at a different point.

Transposition Ciphers Riddle

A transposition cipher changes the position of letters in the plaintext to form the cipher text. For instance, suppose the plaintext is:

<div align="center">X.   EIGHTFOURSEVEN</div>

One way to encrypt it is to write the plaintext evenly divided across three lines, like so (padding it with random letters at the end to make the lines even):

<div align="center">

EIGHT

FOURS

EVENX

</div>

Now read the letters down each column to create the cipher text:

<div align="center">XI.   EFEIOVGUEHRNTSX</div>

Other patterns include spirals, alternating left-to-right and right-to-left rows, and more. Any pattern can work as long as the sender and receiver agree.
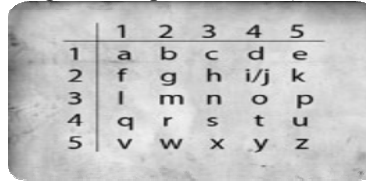
Book Cipher Riddle

A book cipher uses some lengthy text as an encryption key. Common texts include dictionaries, religious books (such as the Bible), government documents (such as the Declaration of Independence), and more. A book cipher encrypts each letter in the plaintext by referencing the same letter at some position in the key document. To encrypt a plaintext letter, replace it with a set of numbers that can be used to locate the letter in the document. A triplet of numbers could indicate the page number, line number, and word number in the line.

Poly-graphic Ciphers Riddle

A poly-graphic cipher is one that uses groups of letters instead of single letters as the basic units of encryption. For instance, AA could be replaced with QJ, AB with RU, etc. With single letters in a simple substitution cipher, there are only 26 possibilities for how each letter is encrypted, but with two-letter groups in a poly- graphic cipher there are 676 possibilities. This makes such ciphers much more difficult to crack.

Polybius Square
Some common poly-graphic ciphers make use of an arrangement of letters known as a Polybius square. The basic square lists the letters in order from left-to-right and top-to-bottom (I and J are treated as the same letter), like this:

Fig .9. Polybius square.

Tap Code
The tap code, which also uses a Polybius square, has been used by prisoners to communicate by tapping on pipes or walls. To encode a letter, a prisoner would tap a number of times equal to the letter row, pausing, then a number of times equal to the letter column, then pausing again. So the word "THE" would be "tap tap tap tap (pause) tap tap tap tap (pause) tap tap (pause) tap tap tap (pause) tap (pause) tap tap tap tap tap".

Play -Fair
Play-fair is a cipher that regularly appears in puzzle caches, cryptic crosswords, and a variety of other contexts. The Play-fair cipher was not invented by Lord Play-fair, but by his friend Charles Wheatstone. While a standard Polybius square has the letters in left-to-right, top-to-bottom order, the Play-fair grid begins with a key word (with duplicate letters removed), then followed by all remaining letters in the alphabet in order. The letter J is not used, and the letter J in the plaintext is replaced with the letter I before encryption. For example, the Play-fair square using the word "CIPHER" as the key would look like this:

Fig 10. Play –Fair Cipher

Four-square Cipher
The four-square cipher uses two key words and four Polybius squares arranged in a 2x2 grid. It is a very strong poly-graphic cipher that corrects a relative weakness in the Play- fair cipher. In Play-fair, if AB encrypts to XY then BA encrypts to YX, so knowing one pair automatically gives you the other pair. In four-square, AB may encrypt to a completely different pair than BA.

XII. CONCLUSION:

We addressed the problem of selective jamming attacks in wireless networks. We considered an internal adversary model in which the jammer is part of the network under attack, thus being aware of the protocol specifications and shared network secrets. We Present two Techniques like Secret technique and Cryptography Riddle. and which are transform a selective jammer to a random one by preventing real-time packet classification. Here we are not presenting the another important Technique lik e AORNT(All Or Nothing) Technique because All-Or- Nothing Transformations (AONT) that introduces a modest communication and computation overhead. Such transformations were originally proposed by Rivest to slow down brute force attacks against block encryption algorithms. AONT serves as a publicly known and completely invertible pre-processing step to a plaintext before it is passed to an ordinary block encryption algorithm. In Next Presentation We may focus on AONT Transformations
Our Techniques combine cryptographic primitives such as commitment schemes, cryptographic puzzles for physical (PHY) layer characteristics.

XIII. FUTURE SCOPE

In the Next Presentation, We may also analyze the security issues of the above said Enhanced Packet delivery techniques .And Also Present the computations Analysis for the Crypto-Logic Riddles.

XIV. REFERENCES:

[1] Alejandro Proãno and Loukas Lazos- Packet- Hiding Methods for Preventing Selective Jamming Attacks.
[2] G. Noubir and G. Lin. Low-power DoS attacks in data wireless lans and bad guys. In DIMACS Workshop on Mobile and Wireless Security, 2004
[3] www.techterms.com/definition/wireless\
[4] http://www.geocaching.com/seek/cache_details.aspx?guid=395a56a3-61b4-4c29-b413-69374d4c2565
[5] Y.Wang, G. Attebury, and B. Ramamurthy. A survey of security issues in wireless sensor ne tworks. IEEE Communications Surveys and Tutorials, 8(2):2–23, 2006.
[6] J. Douceur. The sybil attack. In 1st International Workshop on Peer-to-Peer Systems - IPTPS,2002.
[7] Andrew S. Tanembaum. Redes de computadores. Elsevier, Rio de Janeiro, 4ž edition edition,2003.
[8] www.spamlaws.com/jamming-attacks.html
[9] www.cambridge.org/us/catalogue/
[10] Gustavo S. Quirino, Admilson R. L. Ribeiro and Edward David Moreno- Asymmetric Encryption in WirelessSensor Networks
[11] www.wireless-center.net/Cisco-Wireless-Networking/726.html.
[12] www.nsnam.org/wiki/index.php/Wireless_jamming_model
[13] Le Wang, Alexander M. Wyglinsk-A Combined Approach for Distinguishing Different Types of Jamming Attacks against Wireless Networks