The International Journal Of Engineering And Science (IJES)
||Volume|| 3 ||Issue|| 01 || Pages || 56-63 || 2014 ||
ISSN (e): 2319 – 1813 ISSN (p): 2319 – 1805

# Review on a packet hiding: a new paradigm for avoiding jamming attack over wireless network

Miss Gavali S.B, Mrs. Gavali A.B., Mr.Patil D.S.
Dr. D Y Patil, COE, Ambi, Pune[1,2], ,SBPCOE, Indapur[3], Shriram IET,Paniv[4], India

**----------ABSTRACT----------**

*The wireless network are usually preferred because of its challenging features such as its faster accessibility, compatibility and its connectivity among extended variant set of users. Due to its better transfer rate the authentication mechanism is ignored in wireless sensor network. This shortens the limitation of the existing wired network. By using the wireless sensor network various types of jamming attacks are invited. Some detection strategies are available but they are failed sometime in analyzing and reporting the presence of jammer. In case of external threat model it is quite easy but in case of an internal threat model the person has great knowledge about network secrets and internal protocol specifications, so these persons can easily launch low effort squeeze attacks. These attacks are very difficult to detect and count. So as to protect the packets from such attacks various methodologies are implemented. The main goal of these methodologies is to prevent that packet from the jammer, so as to enable the safe transmission among intended nodes even in presence of jammer.*

***Keywords-*** *Packet hiding schemes, jamming attacks, commitment schemes, overview.*

---

Date of Submission: 06 January 2014 Date of Acceptance: 15 January 2014

---

## I. INTRODUCTION

In wireless network due to its openness nature various intentional interference attacks are comes into existence. Anyone with a transceiver can easily launch jamming attack in an ongoing transmission, or create noise or collision or block the transmission of authorized one or inject spurious messages. One of the best way to degrade the network performance is to jam the wireless transmission or to allow the adversary to take more efforts on jamming the network [1,2]. In the simplest form of jamming, the adversary takes first few bytes of transmitted packet classifies it and corrupt it by causing electromagnetic interference such as magnetic radio waves, FM modulated noise in the network's operational frequencies, and in proximity to the targeted receivers. Under this strategy, jammer includes either continuous or random transmission of high interference signals [3], but due to this it has several disadvantages occurred. The first is that the adversary has to spend its more amount of energy to jam frequency bands of interest and the second one, Due to continuous presence of unusually high interference levels make these types of attacks easy to detect [1,2], [4].

The adversary considered in proposed system is active but only for short period of time. These adversaries target the messages which have more importance. The examples are rout request messages, rout reply messages or the TCP acknowledgement [5]. So the first step of the attacker is that he must be capable of implementing the strategy called as "Classify then jam" before wireless transmission completes.

Suppose there are two communicating parties A (sender) and B (receiver) and J is the jamming node within their communication range. Now A sends packet m to B, the goal of J is takes first few bytes of m classifies them and then corrupt these few bytes. And then visualize to A as J is nothing but B and then start to communicate with A. In this way J requests for more and more packets to A in order to target them for attacking purpose. In this way jammer attacks but the main condition required for the attacker is that he must be knowledgeable at every layer of the TCP protocol. The whole communication is shown in figure 1which gives the actual study of jamming attack.

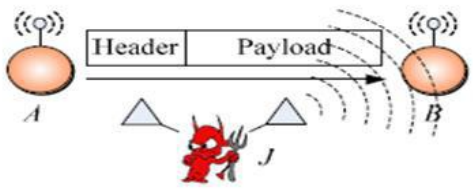


Fig.1. Realization of selective jamming attack

This above all gives information regarding how the attack actually occurred in the wireless network. The steps carried out by the attacker to jam the communication range of A and B. The knowledge required for that attacker. Now we are going to study the actual format for frame in wireless network. The terms used in that frame and the information contained in each term .This format also gives knowledge regarding the optional terms.

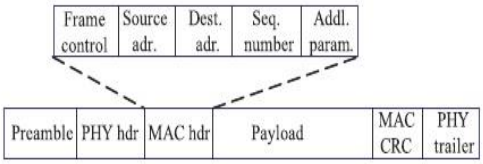


Fig.2 Generic frame format for wireless network

The frame format consists of preamble, PHY-header followed by the payload, then MAC CRC and the PHY-trailer. The MAC header consists of source and the destination address of the packet. The Now we are going to study in detail the use of each term. The first one is the preamble which is used for synchronizing the process at the receiver side. The transmission rate and the length of the frame is defined by PHY-layer header. The third term used is the frame is 'MAC header'. This header includes information such as source and destination address, the version of protocol used, sequence number and some additional fields. The next field is payload which typically contains either ARP packet or an IP datagram. At the last, the cyclic redundancy check (CRC) code is used to protect the MAC frame in order to achieve great security. To maintain the synchronization between sender and receiver the trailer may be appended, at PHY layer.

To investigate the feasibility of real time packet classification for launching selective jamming attack various solutions are provided. The sophisticated adversary considered in proposed system uses the knowledge of network protocol and network secrets extracted from compromised nodes to jam the wireless network. The proposed system develops three schemes in order to mitigate selective jamming, these are as follows that combine cryptographic mechanisms such as cryptographic puzzle scheme [6], strong hiding commitment schemes [7], and all or nothing transformations [8], with physical layer parameters.

We further study the effect of various selective jamming strategies on the network performance. The remainder of this paper is organized as follows. The section II represents the study of related work with its disadvantages. In section III, we are going to study the problem statement of the proposed system and assumptions used. In section IV, we illustrate the impact of selective jamming at the transport and network layer. In section V, represents the proposed system and its advantages. In section VI, we study the methods that are used for preventing the selective jamming. In section VII, illustrates the Implementation of working steps. In section VIII we conclude.

## II. RELATED WORK

In related work we are going to study the reasons for jamming, the requirements for it, whether it happens intentionally or intentionally. At the last we are going to study about spread spectrum technique which is used by conventional anti-jamming methods and the disadvantages of existing system, the mechanism for prevention they used.

Due to jamming wireless transmission either stopped or disturbed. This jamming is either in the form of interference, noise or collision. If the jamming is intentionally then it is in the form of attack otherwise it is caused due to network load. No any special hardware required for executing it. Conventional anti-jamming techniques are based on either some form of jamming evasion or SS communications [3], [9]. Now we are going to study in detail about Spread Spectrum (SS) communications.

Spread spectrum communications works as follows. First the input is given to channel encoder, now the channel encoder creates analog signal which consist of narrow bandwidth. Now this generated signal is modulated by using the sequence of digits. Pseudo noise or pseudo-random number generator is the main source for generating the Spreading code. The main reason for using 'modulation' mechanism is to increase signal's bandwidth which is going to be transmitted. This whole procedure is carried at the sender side. Now at the receiver side for demodulating the spread spectrum signal digital sequence is used. This generated signal is given to channel decoder in order to recover the original data. Spread spectrum is generally used for hiding and encrypting signals.

However, compromise of PN nodes that are commonly shared neutralizes the advantages of SS in case of broadcast communication [17]. Popper proposed one anti jamming model which is used only for pairwise communication. It does not allow any shared secrets. For broadcast communication Popper uses PN nodes to provide bit level protection [3].

Some existing system allows only probabilistic analysis of how the collision or interference occurred; it does not deal with prevention mechanism. Some gives only overview of jamming attack. Some focuses on protection of jamming attack under an external threat model but in case of internal threat model the single node is sufficient for revealing the relevant information. The other disadvantage is that adversary uses high interference signal. Also the adversary has to spend more amount of time to jam the frequency band of interest.

## III. PROBLEM STATEMENT AND ASSUMPTIONS

Under this chapter we are going to study the actual problem statement of the proposed system and the various kinds of assumptions made by the system for the understanding purpose.

### *A. Problem Statement*

Consider the scenario depicted in Figure 1. 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 these few bytes by interfering between their communication and viewing A that J is nothing but B and then start to communicate with A for corrupting the messages received from A. We address the problem of preventing the jamming node from classifying m in real time, thus mitigating J's ability to perform selective jamming. The main goal of the proposed system is to transform a selective jammer to a random one.

### *B. Network Model*

The network consists of collection of nodes connected via wireless links. In our proposed system we are considered 12 nodes that are communicate directly if they are within their communication range or they can use multiple hops. The communication of these nodes is carried out by various types of modes. They can communicate in unicast mode by using simplex link or bicast mode by using duplex link or in broadcast mode. Communication is kept either in encrypted format or in unencrypted format depending on the prevention scheme used. In case of broadcast communication the symmetric keys are shared among all intended receivers which are generated by asymmetric cryptography or pre-shared pairwise keys.

### *C. Communication Model*

In communication model various symbols are used and each symbol has special meaning. The packets are transmitted over network at the rate of R bauds. Each symbol in PHY layer corresponds to q bits. This q is defined by digital modulation scheme. Every symbol carries $\alpha/\beta$ q data bits, where $\alpha/\beta$ is the rate of the PHY-layer encoder. Here two types of bit rates are used. The one is transmission bit rate which is equal to qR bps and the other is information bit rate which is $\alpha/\beta$ qR bps. To protect the wireless transmission from jamming at the PHY layer the SS technique uses frequency hopping or direct sequencing. SS provides immunity to interference to some extent (typically 20 to 30 Db gain), but a jammer which is very powerful is still capable of jamming data packets chosen by him.

## IV. IMPACT OF SELECTIVE JAMMING

In this section we are going to illustrate the impact of selective jamming on the network performance. To implement jamming attacks, the proposed system uses Network Simulator 2.34. Here the two wireless network scenarios are considered. In the first scenario the attacker targeted TCP connection especially at the transport layer. The second scenario, the jammer focuses on network-layer control messages which are transmitted during the route establishment process.

### *A. Selective Jamming at the Transport Layer*

In this experiment, we set up transfer of 3 MB file between two users A and B connected via multi-hop route. The TCP protocol was used for reliable connection. The RTS/CTS mechanism was enabled at the MAC layer. Here the transmission rate 11Mbps was considered at each link. The jammer was placed within communication range of A and B. various selective jamming strategies were considered here, 1.Selective jamming of cumulative TCP-ACKS. 2. Jamming of any data packet. 3. Random jamming. 4. Jamming at MAC layer means RTS/CTS messages. In each of these strategies fraction p is jammed. This fraction p is of the targeted packet.

### *B. Selective Jamming at the Network Layer*

In this scenario, 12 nodes of multi-hop wireless networks are simulated randomly within the square area. Here AODV routing protocol is used in proposed system for establishing and discovering the routing path for the data packets. Connections are established between source/destination pairs. In this scenario the jammers are placed in non-overlapping area of the network. In proposed system continuous, random and targeted RREQ these types of jammers are considered that block the fraction p of targeted packet. Constant jamming attack is equally effective to attack on RREQ messages. However, selective jamming is several orders of magnitude more efficient. But due to flooding process of AODV random jammer fails to disturb route paths.

## V. PROPOSED SYSTEM

This chapter describes the brief introduction of proposed system. The way that proposed system provides security and the advantages of it over existing systems. Proposed system provides intuitive solution against jamming by encrypting the entire packet along with the header. For generating the cipher text static key is used. The static decryption key is shared among all intended receivers in case of broadcast communication. Though we kept encryption key secret, but static portion of packet which has been transmitted can be used for packet classification. This is one of the advantages of proposed system.

The main advantages of proposed systems are- It is very easy for exploiting knowledge of protocol and cryptographic primitives extracted from compromised nodes. The other main advantage is that the proposed system shows that selective jamming attacks lead to DOS by taking very less effort on behalf of jammer. In this way the proposed system achieves strong security protocols.

## VI. METHODS USED

There are various methods that are used for achieving strong security of system we will go through them in detail. We will first study how the jammer performs attack on the system with the help of real time packet classification then we will further study the various cryptographic schemes that prevent these jamming attacks.

### *A. Real time packet classification*

At the physical layer packet m is encoded, interleaved and modulated before it is reached at the receiver side. This whole procedure is carried out at the sender side. Now, at the receiver side same process is done but in reverse format like first demodulation is carried out then that packet is de- interleaved and then at last demodulation is done so as to get the original packet at the receiver side as shown in figure 3. Between two communicating parties there is jamming node J which classifies first few bytes of m corrupts them and then view sender as it is a receiver for launching more attacks.

### *B. Strong hiding commitment scheme*

In this scheme, Symmetric encryption technique [10] is used in which static key is shared between two communicating parties before actual communication starts.

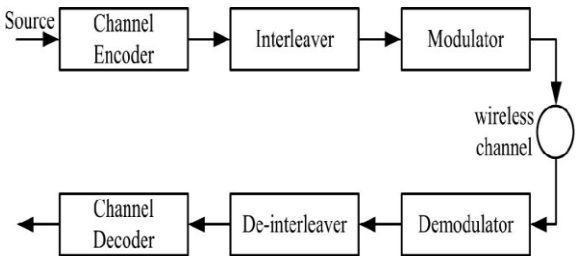


Fig.3. Generic communication system diagram

By using that key sender encrypts the data and sends it to the receiver side and at the receiver side, receiver decrypts the cipher text so as to get the original plain text [11].Consider sender S constructs commit message with the help of permutation key and key k is chosen of random length. At the receiver side any receiver R computes by receiving d (de commit message).

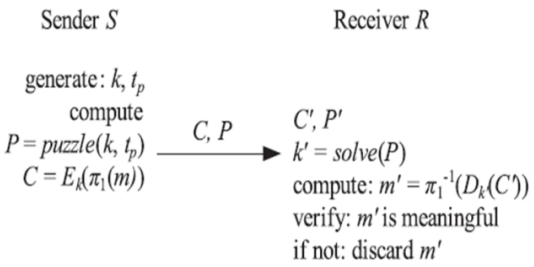


Fig.4. Cryptographic puzzle hiding scheme

The encryption of whole transmitted packet including header also is best solution against jamming. Hence the proposed system uses it but the problem arises in case of broadcast communication because the decryption key must have to share among all intended receivers which can be susceptible to compromise. When adversary found decryption key it starts decrypting it without waiting for first cipher text block. Here we are considering the cipher block chaining (CBC) concept, to encrypt a message m with a key k and an initialization vector IV is set, message m is split into x blocks m1, m2, . . . mx, and each cipher text block ci, is generated as

$c1=IV, ci+1= Ek (ci \oplus mi)$ $i= 1, 2,. . , x$ (1)

Where Ek(m) denotes the encryption of m with key k.
The plaintext mi is recovered by

$mi= ci \oplus Di(ci+1)$ where $i=1,2,\ldots,x$ (2)

From equation (2) the reception of ci+1 is sufficient for recovering the original packet mi if k is known (c1=IV is also known). Therefore, real time packet classification is still possible. One solution to the key compromise problem would be to update the static key time to time whenever it is compromised. However, such a solution is not useful if we generate new key from compromised node. The key compromise problem can be avoided by using the mechanism that identifies compromised set of nodes.

### *C. Cryptographic puzzle hiding scheme*

As the name suggests it is based on puzzle creation and solving it. As shown in figure 4, sender S generates puzzle p in which k is the key and tp is time required to solve that puzzle [12]. In this way at the sender side puzzle P along with cipher text C (which is created by first message or packet is permutated and then it is encrypted with the key) is generated and they are sending to the receiver side. At the receiver side puzzle is solved and key is generated and by using that key the receiver will get the message if it is equal to m' then that message will kept as original otherwise that message is discarded [15]. We can use hash based puzzle technique also in which Client puzzles uses one-way hash functions with partially disclosed inputs to force puzzle solvers search through a space of a precisely controlled size.Here the concept of time lock puzzle is used we will study it in detail.

- *Time-Lock Puzzles*

Rivest had proposed a mechanism which is called as time lock puzzles. These are mostly relying on modulo operations which are controlled and they are performed iteratively. Time lock puzzles provide fine granularity over tp. It also gives sequence nature of the computation also it requires very less time for computation as compare to puzzle solving. Due to these attracting features Time lock puzzle is mostly used.

In time lock puzzle, the puzzle P consist values, P= (g, Kh, t, a). At first puzzle constructor generates a composite modulus g= u. v, where u and v are two large random prime numbers. Here a is random number and the condition requires $1<a<g$. And the encryption key is hidden in Kh, such that $Kh=k+a^{2t} \bmod g$, where t=tp. This whole process is done at puzzle generator/sender side. Now at the puzzle solver side, N is the time required to solve that puzzle. Here the assumption is made as solver can perform N squaring modulo g per second. The encryption key k hidden under Kh is computed easily if factorization of g are known or $\phi(g) = (u-1).(v-1)$.Otherwise a solver have to perform all t squaring to recover k.

### *D. Hiding based on All-Or-Nothing Transformation*

Under this cryptographic scheme we are going to study Linear AONT and Hiding sub layer details. Under this scheme packets are only preprocessed before sending it receiver side. Likewise other methods here the packets are not encrypted. In this scheme the jammer can't perform packet classification until all pseudo messages corresponding to original packet have been received and inverse transmission applies. In our context function f is generated .In that function packet m is partitioned to a set of x input blocks m = (m1, m2,…, mx}, which serve as an input to an AONT

$f : \{IFu\}^{x} \rightarrow \{IFu\}^{x'}$

Here, IFu denotes the alphabet of blocks mi and $^{x'}$ denotes the number of output pseudo messages with $x' \geq x$. The set of pseudo messages m'={m'1,m'2,…..m'x'} is transmitted over the wireless medium. At the receiver, the inverse transformation f ^-1 is applied after all x' pseudo messages are received in order to recover m.

- *Linear AONT*

To construct a linear AONT the alphabet of the input blocks is a finite field IFu, with the order u being a prime power. He showed that if an invertible matrix M={mijImij ε IFu , mij≠0 }x×x exists, then the transformation f(m)=mM^-1 is a linear AONT.

- *Hiding Sub layer Details*

As the name suggests this scheme is based on hiding sub layer placed between MAC and PHY layer. In the initial step, message m is padded so as to adjust frame length. The padding operation is done by using pad(). Due to padding done early there is no need to pad at the PHY layer. And also length of m becomes multiple of length of pseudo messages m'i. This will ensure that all bits of the transmitted packet are part of the AONT. In the next step, m ‖ pad(m) is partitioned to x blocks, and the AONT f is applied. Message m' is delivered to the PHY layer. At the receiver, the inverse transformation f^-1 is applied so as to obtain m ‖ pad(m). The padded bits are removed and the original message m is recovered.

## VII. IMPLEMENTATION STEPS

The figure 5 shows detail implementation of the proposed system with its analysis and throughput. There are following steps carried out to perform the implementations these are as follows.

- Implementation of wireless node in NS-2 with AODV.
- Implementation of jamming attack with selective transmission.
- Implementation of packet classification for wireless traffic.
- Implementation of packet hiding for real packet.
- Detection of jamming attack and analysis with throughput.

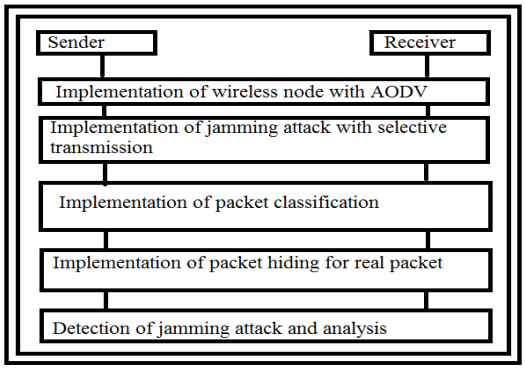


Fig.5.Generic diagram for proposed system

In the first step we are establishing the connection between nodes over wireless network. The 12 nodes are considered in the proposed system. They are communicated with each other either by using simplex link or duplex link. The transmission rate is 11 Mbps. In the second step we are implementing the jamming attack, for that we are using trace file. This file consists of all information related to the packet for example source address, destination address, the length of the packet, the sequence number and some additional terms. In the third step real time packet classification is done. For that each attribute at the physical layer must be known with its purpose. In the next step we are hiding the packet from the jammer so that strong security can be achieved.

At the last step detection of jamming attack is done, this step must be performed carefully. By implementing these steps the proposed system produces the required result. Now two ratios PDR and PSR are determined for comparative analysis. In this way proposed system works.

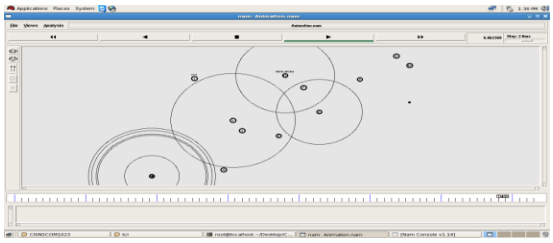

Fig.6. Communication of wireless node

The figure 6 shows communication of wireless nodes. This screenshot is support software of NS2.This is used for visualization which is called as Nam. This file is specially used for viewing network simulation traces and real world packet trace data. It is also called as network animator. It visualizes topology layout, various data inspection tools and packet level animation. Before working with Nam file first we have to create trace file that should consists of topology information for example nodes, links, packet traces.

During an NS2 simulation, user can produce topology configurations, layout information and packet traces with the help of tracing events in NS2. When the trace file is generated, it is ready to be animated by Nam. Upon startup, Nam will read the trace file, create topology, pop up a window, do layout if it is necessary and then pause at the time of the first packet in the trace file. Nam provides control over many aspects of animation through its user interface. Nam does animation using the following building blocks: node, link, queue, packet, agent and monitor.

- *Packet Send Ratio (PSR):*

Wireless device measures PSR ratio easily for keeping track of number of packets it wants to send and the number of packets that are sent successfully. The ratio of packets that are successfully sent out by a trusted traffic source compared to the number of packets it wants to send out at the MAC layer is nothing but PSR [21]. Suppose *A* has a packet to send. Before performing transmission many wireless networks employ some form of carrier-sensing multiple access control. For example, in the MAC protocol, the channel must be sensed as being in an idle state for at least some random amount of time before A can send out a packet.

Further, there are various types of MAC protocols that have various definitions on an idle channel. Some simply compare the signal strength measured with a fixed threshold, while others may adapt the threshold based on the noise level on the channel. A radio interference attack may cause the channel to be sensed as busy, causing *A*'s transmission to be delayed. If too many packets are buffered in the MAC layer, the newly arrived packets will be dropped. It is also possible that a packet stays in the MAC layer for too long, resulting in a timeout and packets being discarded. If *A* intends to send out *n* messages, but only *m* of them go through, the PSR is *m/n.*

- *Packet Delivery Ratio (PDR):*

The ratio of packets that are successfully delivered to a destination compared to the number of packets that have been sent out by the sender [21]. Even after the packet is sent out by *A*, *B* may not be able to decode it correctly, due to the interference introduced by *X*. Such a scenario is an unsuccessful delivery. The PDR can be measured at the sender or receiver side. The PDR may be measured at the receiver *B* by calculating the ratio of the number of packets that pass the CRC check with respect to the number of packets (or preambles) received. PDR may also be calculated at the sender *A* by having *B* send back an acknowledge packet. In either case, if no packets are received, the PDR is defined to be 0.

## VIII. CONCLUSION

This paper solves the problem of selective jamming attacks in wireless network. Here an internal threat model is considered in which the jammer is part of the network, thus being aware of the protocol specifications and network secrets. Jammer can classify transmitted packet in real time by decoding the first few symbols of an ongoing transmission or packet. We evaluated the impact of selective jamming attacks on network protocol such as on TCP and routing. This paper developed three schemes that transform a selective jammer to a random one by preventing real time packet classification. These schemes combine cryptographic primitives such as commitment schemes, cryptographic puzzles, and all-or-nothing transformations with physical-layer characteristics. We analyze the security of our method and quantified their computational and communication overhead.

## REFERENCES


[1] W.Xu, W. Trappe,Y.Zhang,andT.Wood, "The feasibility of launching and detecting jamming attack in wireless network",Proc.ACM Int'l Symp. Mobile adhoc networking and computing (MobiHoc),pp 46-57,2005.

[2] W. Xu, T. Wood, W. Trappe, and Y. Zhang "Channel surfing and spatial retreats: Defenses against Wireless denial of service", Proc. Third ACM workshop wireless security, pp.80-89, 2004.

[3] M.K.Simon, J.K.Omura, R.A.Schotlz, and B.K.Levitt, Spread spectrum communications Handbook. McGraw-Hill, 2001.

[4] G.Noubir and G.Lin.Low power DoS attacks in data wireless LANs and countermeasures,ACM SIGMOBILE Mobile computing and communications Review,7(3):29-30,2003.

[5] C.Po"pper, M.Strasser,and S._capkun "Jamming-Resistant Broadcast communication without shared keys", Proc. USENIX security Symposium., 2009.

[6] Juels and J.Brainard. Client puzzles: A cryptographic countermeasure against connection depletion attacks. In proceedings of the network and distributed System Security Symposium, pages 151-165, 1999.

[7] Damgard.Commitment schemes and zero knowledge protocols,Lecture notes in computer science, 1561:63-86.

[8] R.Rivest. All-or-Nothing encryption and the packet transform. Lecture notes in computer science, pages 210-218, and 1997.

[9] Y.Desmedt,"Broadcast Anti-jamming Systems", Computer Networks, vol.35,nos.2/3, pp.223-236, Feb.2001.

[10] D.Stinson. *Cryptography: Theory and practice.* CRC press, 2006.

[11] Dilip Kumar D.P 1, H.Venugopal2. Avoiding selective jam attack by packet hiding method in wireless sensor network.

[12] K.Manojkumar, M.Vinothkumar, and Dr.G.TholkappiaArasu, An Analysis on Denial of Service attacks and packet defending methodologies in wireless sensor network.

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

[14] StefaniaSesia, IssamToufik, and matthewBaker,editors,LTE, UMTS Long Term Evolution:From Theory to Practice,chapter9.John Wiley & Sons Ltd,Chichester, second edition,2011.

[15] ShabnamSodagariand T.CharlesClancy,Efficient jamming attack on MIMO channels, VA, USA.

[16] OPNET http://www.opnet.com/solution/network rd/modeler.html.

[17] GeethapriyaThamilarasu, Sumita Mishra and RamlingamShridhar, Improving reliability of jamming attack detection in Ad hoc networks, IJCNIS, vol. 3,No.1,April 2011.

[18] Kwangsungju and Kwangsue Chung, Jamming attack detection and rate adaptation Scheme for IEEE 802.11Multi-hop Tactical networks, vol. 6, April 2011.

[19] MingyanLi,Iordamiskoutsopoulosand radhapoovendran,Optimal Jamming Attacks and network Defense Policies in Wireless Sensor networks,infocom,2007

[20] Alejandro Proano and LoukasLazos, Selective Jamming Attacks in Wireless Networks,Dept of Electrical and Computer Engineering University of Arizona.

[21] WenyuanXu, Wade Trappe, Yanyong Zhang Timothy Wood,The Feasibility of Launching and Detecting Jamming Attacks in Wireless Networks.

[22] S.Jiang and Y.Xue(Eds.), Optimal Wireless Network Restoration under Jamming Attack,Proceedings of 18th International Conference on Computer Communications and Networks,California.

[23] P.Tague,M.Li, and R.Poovendran .Probabilistic mitigation of control channel jamming via random key distribution.In*proceeding of the PIMRC*,2007.