ISSN:0975-9646

# Prevention of Selective Jamming Attack Using Cryptographic Packet Hiding Methods

S.B.Gavali [1], A. K. Bongale [2] and A.B.Gavali[3]

[1]*Department of Computer Engineering,*
*Dr.D.Y.Patil College of Engineering, University of Pune, Ambi, Pune, India*

[2]*Asst. Professor, Department of Computer Engineering,*
*Dr. D.Y. Patil College of Engineering, University of Pune, Ambi, Pune, India*

[3]*Asst. Professor, Department of Computer Engineering,*
*S.B. Patil College of Engineering, University of Pune, Indapur, Pune, India*

**Abstract-The wireless medium provides various challenging features among various set of users due to its sharing nature. It provides better transfer rate but authentication is ignored and it is very important in real world. This minimizes the limitation of existing wired network. These networks act as launch pad for various types of jamming attacks. Various methodologies are available but sometime they fail in analysis and detection of jamming attack. The analysis and reporting of jamming attack is quite easy in case of external threat model but in terms of internal threat model it is very difficult, these internal adversaries uses the knowledge about network secrets and network protocols to launch squeeze attacks with very low effort. To prevent these attacks various cryptographic schemes are implemented. The main goal of these systems is to prevent the preserved information at the wireless physical layer and allowed the safe transmission among communicated nodes although the jammer is present.**

**Keywords-Commitment scheme, Network Protocols, Packet hiding methods, Real time packet classification and Selective jamming attacks.**

## 1. INTRODUCTION

The wireless medium provides faster accessibility, compatibility and connectivity between different users. Though it provides features but various types of attacks are invited because of its sharing medium. The adversaries with internal knowledge of network secrets take more effort on jamming the network or degrade the network performance [14], [15]. Anyone which has transceiver can easily inject spurious messages or create noise or interference or launch jamming attack in an ongoing transmission or block the transmission of legitimate users. In the simplest form, the jammer classifies first few bytes of transmitted packet and corrupts them by creating proximity of the targeted receivers or FM modulated noise or electromagnetic interference such as magnetic radio waves.

In these schemes, jammer includes either continuous or random transmission of high interference signals [10], [11], and cause several disadvantages as, first 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 [6],[14], [15].The adversaries are active only for short period and targeting the message of high importance for example rout request, rout reply messages or TCP acknowledgement [2]. Before the wireless transmission completes, the very basic step of the jammer is to implement "Classify them jam" strategy [1].

Consider the communication of nodes as A (source node) and B (destination node) and J is the jamming node within their communication range. Now A sends packet or message m to B, the goal of J is classifies first few bytes of transmitted packet, then corrupt these few bytes and view to A as J is nothing but B ( proximity of targeted receiver).The figure 1 gives the realization of jamming attack.

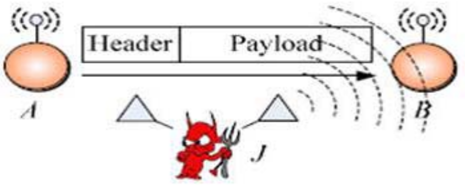

Figure 1. Realization of selective jamming attack

Jammer must have knowledge about each layer of the TCP protocol, is the required condition [1].The actual format for frame in wireless network as shown in figure 2. The preamble, PHY-header, MAC header, payload followed by MAC CRC and the PHY-trailer which might be optional, these are the terms used in the frame format. The trailer may be appended at PHY layer to maintain the synchronization between sender and receiver [2].To jam the network, the sophisticated adversary uses the knowledge of network protocol and secrets extracted from compromised nodes.

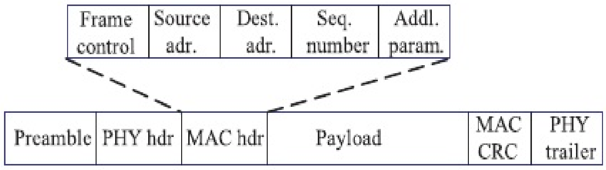

Figure 2. Generic frame format for wireless network

The three schemes are developed in order to mitigate these attacks. These are as follows that combine cryptographic mechanisms such as strong hiding commitment schemes [4], cryptographic puzzle scheme [8], and all or nothing transformations [12], with physical layer attributes.

The remaining paper is organized as follows. We are representing the existing system with its disadvantages and the cryptographic schemes in the section II. Proposed system and its advantages are studied in section III. We are illustrating the actual implementation in section IV. At the last of paper we are studying the results generated by proposed system in section V and in section VI we conclude.

## 2. Background Work

In related work, we are studying the reasons for jamming, spread spectrum techniques used by the conventional systems and the disadvantages of existing system, prevention mechanism they used and at the last we are studying how the real time packet classification is performed and strong hiding commitment scheme which is used by our proposed system.

Because of jamming, the wireless network either stopped or disturbed. Noise, collision, interference these are various forms of jamming. Jamming may be performed intentionally or unintentionally, depending upon either performing attack or due to network load. There is no need of special hardware to execute these attacks only knowledge of preserved information is required.

Conventional systems are using spread spectrum communication or some jamming evasion [11], [15]. Now, we see how the Spread spectrum technique actually works. First input is given to channel encoder for creating analog signal having narrow bandwidth. The next step is performing modulation for increasing signal's bandwidth that going to be transmit with the help of sequence of digits. The spreading code is generated by either pseudo noise or pseudo-random number generator. Now at the receiver side digital sequence is used for demodulation and then decoding is carried out to recover original data. SS technique is used for hiding and encrypting signal. But in case of broadcast communication compromise of single PN node neutralizes advantages of SS [9].

Existing system more focused in case of external threat model but in case of internal threat model the compromise of single node is sufficient for getting useful information. Some existing system gives only probabilistic analysis about collision or interference. Some give overview of jamming attack with poor security. The other disadvantages are unusually use of high interference level make these attacks easy for detection also adversary have to spend more energy to jam frequency band of interest.

We will first study how the real time packet classification is performed and then we will further study strong hiding commitment scheme for preventing the attacks which is used in proposed system.

### A. *Real time packet classification*

At first the packet m is encoded for creating narrow bandwidth analog signal then it is interleaved and then modulation is performed by using digital sequence. Now, at the receiver side first demodulation then de-interleaving and at the last decoding is done to get original packet as shown in figure 3.

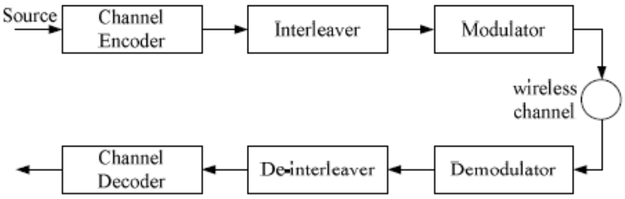

Figure 3. Generic communication system diagram

### B. *Strong hiding commitment scheme*

Under this scheme, one static key is shared between intended pairs before communication starts; this is nothing but Symmetric encryption technique [3]. At the sender side the shared key is used for encryption while at the receiver side it is used for decryption of cipher-text to get the original plain text. In this way sender S constructs commit message by using permutation key and key k of random length [5]. At the receiver side any receiver R can computes by receiving d (de commit message) [7].

The symmetric encryption technique is intuitive solution for jamming attack. Problem is occurred in case of broadcast communication because the static decryption key is shared between all legitimate users causes compromise of single node is sufficient for attacking. By knowing the decryption key adversary start for decryption without waiting for first cipher block. For encryption cipher block chaining (CBC) is used. A message m with key k and initialization vector IV is set, message m is split into x blocks as$m_1$, $m_2$ . . . $m_x$, as $m_i$ and each cipher text block $c_i$, is generated as

$$C_1=IV,\ C_{i+1}=E_k\,(C_i\oplus m_i)\ where\ i=1,2,\ldots,x \qquad (1)$$

Where $\oplus$ is exclusive OR function and $E_k$ (m) denotes the encryption of m with key k, the plaintext $m_i$ is recovered by

$$m_i=C_i\ \oplus D_i\,(C_{i+1})\ where\ i=1,2,\ldots,x \qquad (2)$$

From equation 2 if k is known ($C_1$=IV is also known) the reception of $C_{i+1}$is sufficient for generating the original packet mi. Therefore, real time packet classification is still possible. If the key is compromised then it must have to update from time to time. But it will not be a proper solution if that key is generated from compromised node. One solution to the key compromise problem would be to update the static key time to time whenever it is compromised. The best solution for this key compromise problem is that identify a mechanism that find set of compromised nodes.

## 3. Proposed System

Proposed system gives brief introduction along with its advantages. It gives best solution for jamming by using strong hiding commitment scheme, for that entire packet with header is encrypted for generating cipher text. Even though encryption key remain secret its static portion is allowed for classification of packets. In broadcast communication the static decryption key must be shared between intended nodes.

There are some advantages of proposed system- Very easy for exploiting knowledge from compromised nodes. The second advantage is that proposed system gives selective jamming attack to DOS with very low effort. By using proposed system strong security protocols are achieved.

## 4. Actual Implementation

Proposed system uses Network Simulator 2.34 tool in which front end is tcl and back end is c++. Here two protocols are used. TCP protocol is used for establishing reliable connection and AODV routing protocol is used for finding routing path for data packets. The RTS/CTS mechanism enabled at MAC layer. The transmission rate is 11Mbps for every link. The continuous, random, targeted RREQ these jammers are kept between the communicated pairs. But due to flooding feature of AODV the random jammer fails in disturbing route path. The below figure 4 gives the exact flow of the proposed system.

- 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.
-

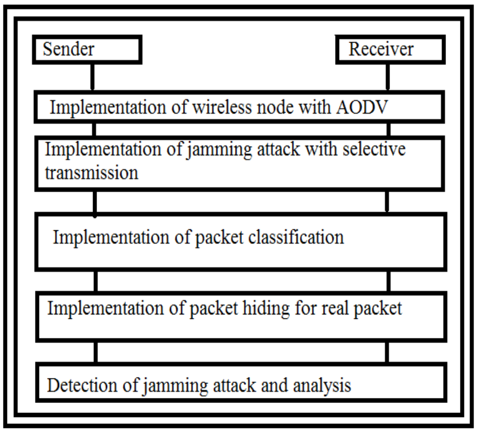
Sender
Receiver
Implementation of wireless node with AODV
Implementation of jamming attack with selective transmission
Implementation of packet classification
Implementation of packet hiding for real packet
Detection of jamming attack and analysis

Figure 4. Generic diagram for proposed system

We are generating communication of 12 wireless nodes in the initial step. AODV routing protocol is used .For establishing the connection using NS2 tool .tcl file is created which gives sequence number and length of the packet, source and destination address and also contains additional fields shown in figure 5.

By compiling the tcl file two files are automatically generated NAM and tr. The NAM file gives information regarding the real world packet trace data, topology information, packet level animation, data inspection tool.

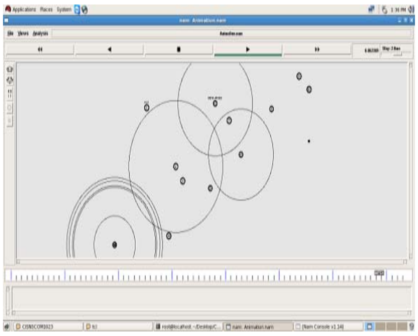

Figure 5. Communication of wireless node

In the second step we are implementing the jamming attack [13]. The ddos.o attack file is generated. After compiling the tcl file of the second step, the PSR and PDR these two graphs and one nam file is generated. The nam file shows how the packets are transmitted between intended nodes and how the jammer node is intruded between them. The PSR graph shows the packet sent ratio versus time as shown in figure 6.

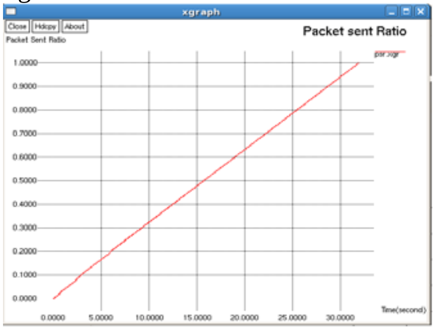

Figure 6. Graph for packet sent ratio

The PDR graph shows how the packets are delivered versus time, as jamming attack is implemented here so the PDR minimizes from 0 to 1 shown in figure 7.

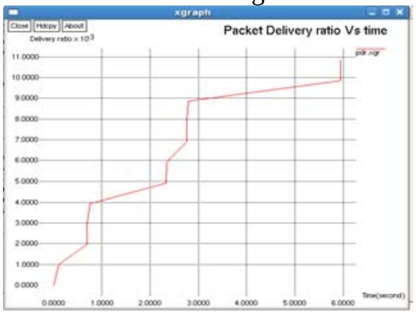

Figure 7. Graph for packet delivery ratio

Our goal is to perform real time packet classification in the third step, each attribute at the physical layer must be known with its use. Here two graphs are calculated for determining Jamming probability Vs Number of packets jammed and Jamming probability Vs Throughput. As the Jamming probability increases the number of packets increases and throughput of the system decreases as shown in figure 8 and 9. In the next step we are hiding the packets of high importance or which we want to transmit between intended nodes by using Hash based encryption and DES algorithm. At the last step jamming attacks are detected and the packets are discarded that are transmitted from the jammer node, this step must be performed carefully. By implementing the last step we can get PDR indicating that the attack is removed also we are calculated the throughputs over different links such as 5-0, 4-7, and 6-8 as shown in figure 10. The proposed system produces the required result so as to achieve great security.

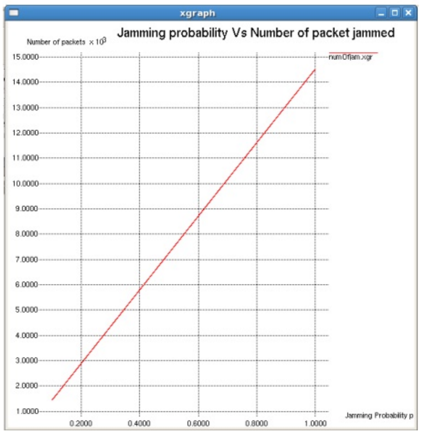

Figure 8. Jamming probability Vs Number of packets jammed

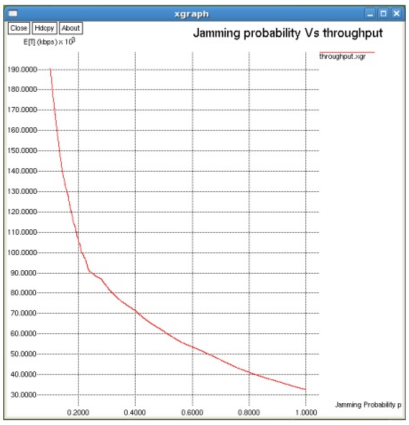

Figure 9. Jamming probability Vs throughput

## 5. Results

In this chapter we are studying data set and result sets and the definition of PSR and PDR also.

- ***Data set***

In the proposed system, 10 nodes source, destination and jammer node are simulated by using NS2.The packets are transmitted from source to destination; this is data set of our proposed system.

- ***Result set***

The result is generated in terms of various graphs PSR, PDR, Jamming probability versus number of packets jammed and jamming probability versus throughput. PSR graph is linear, now due to jamming attack is implemented as ddos.o in Makefile.in as configured. The PDR graph is non-linear. Now when we are performing classification of the real packets from jammed packet at that time we are calculating the number of packets jammed and the throughput of the proposed system which is decreases due to attack from the jammer. At the last step we are hiding the real packets by using cryptographic schemes such as Hash based encryption and DES algorithm. In hash based encryption we are sending the packet or message in encrypted format with hash based value that is pre-shared before actual communication starts and at the receiver side the message is decrypted with the help of hashing value. In DES algorithm at the sender side input is given as plain text and 64 bit key from that the cipher text of 64 bit block is generated. Now at the receiver side DES decryption consists of the encryption algorithm with the same key but reversed key schedule. In this way proposed system avoids the jamming attack over wireless network with great security.

- ***Packet Send Ratio (PSR)***

The PSR is used for measuring how much number of packets want to send and how much of them are sent. The PSR is defined as 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 [15]. Suppose *A* has a packet to send. Before performing transmission many wireless networks employ some form of carrier-sensing multiple access control. A radio interference attack causes the channel to be sensed as busy, causing *A*'s transmission to be delayed. It can be happened that a packet stays in the MAC layer for too long, resulting in a timeout and packets being discarded. If there are so many packets are buffered in the MAC layer, the newly arrived packets will be dropped. 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 PDR is defined as packets that are successfully delivered to a destination compared to the number of packets that have been sent out by the sender [15]. Because of interference entered by X, even if packet is sent out by *A*, *B* may not be able to decode it correctly. This scenario shows an unsuccessful delivery. The PDR can be measured by two ways, the sender or receiver side. At the receiver *B* by calculating the ratio of the number of packets that pass the CRC check per 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.

This PSR and PDR are calculated by using back end using c++.Also encryption and decryption is done at the back end. The figure 10 shows the final result in which throughput of the proposed system is great because of achieving the strong security.

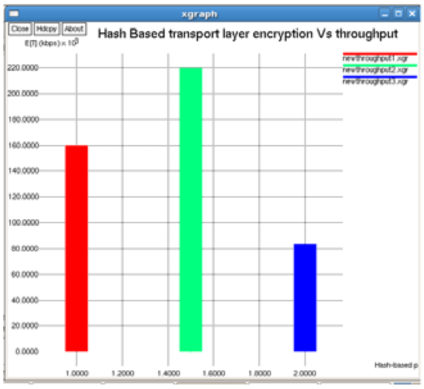

Figure 10. Hash based encryption Vs throughput

## 6. CONCLUSION

This paper provides solution for jamming attack over wireless network. In this paper the internal threat model is considered, in which jammer is part of network and he is aware of network secrets and protocol specification. Jammer can perform classification in real time by decoding first few bytes of the transmitted packet. To prevent real time packet classification various schemes are developed. These schemes combine cryptographic primitives such as strong hiding commitment scheme with physical-layer characteristics so as to transform jammer to random one. We also measured how each jammer fared by their effect on the packet send ratio and packet delivery ratio. We analyse the security of our method and quantified their computational and communication overhead.

## ACKNOWLEDGEMENT

My heartfelt thanks go to Dr. D. Y. Patil, College Of Engineering, Ambi for providing a moral support to develop my skills. I am especially grateful to my guide and respected teachers for their expertise and encouragement. Last but not the least I would like to thanks all those who directly or indirectly provide their overwhelming support during the development of the report.

## REFERENCES

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

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

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

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

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

[6] 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.

[7] Geethapriya Thamilarasu, Sumita Mishra and Ramlingam Shridhar, “Improving reliability of jamming attack detection in Ad hoc networks”, IJCNIS, vol. 3, No.1, April 2011.

[8] Juels and J. Brainard. “Client puzzles: A cryptographic countermeasure against connection depletion attacks (Periodical style-Accepted for publication)”, *the network and distributed System Security Symposium,* to be published.

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

[10] L. Lazos, S. Liu and M. Krunz. “Mitigating control channel jamming attacks in multi-channel ad hoc networks (Periodical style-Accepted for publication)”, *the second ACM conference on wireless network security,* to be published.

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

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

[13] Shabnam Sodagari and T. Charles Clancy, “Efficient jamming attack on MIMO channels”, VA, USA.

[14] 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.

[15] W. Xu, W. Trappe, Y. Zhang and T. Wood, “The feasibility of launching and detecting jamming attack in wireless network”, Proc. ACM Int’l Symposium. Mobile ad-hoc networking and computing (Mobi-Hoc), pp. 46-57, 2005.