Enhanced Packet Dissembling Schemes for Selective Jamming Attacks Prevention in Wireless Networks

Pushphas Chaturvedi *, Kunal Gupta*

Department Of Computer Science, ASET, Amity University

Abstract- Wireless networks provide wide range of services which is never so easy by any other medium, its mode of working tends it to have many security breaches. In modern era of communication trillions of profitable vital information is available on internet and they are accessible through this open medium. Such vital information can be achieved through intentional interference or jamming. In this paper we are trying to provide some efficient techniques which conceal such messages of high importance through dissembling. Dissembling refers to conceal under false appearance, there are various methods of concealing important messages but we tried to use very efficient ones, as messages are dissembled, the jammer won't be able to access it because transaction will be completed before jammer reaches the original important message.

Index Terms- Jamming attacks, Dissembling, Selective jamming, Dissembling commitment scheme, Puzzle dissembling scheme.

I. INTRODUCTION

Wireless network is now very wide area of research because despite of several advantages it has many flaws. Intentional interference attacks are made to jam channel by triggering many page requests or any other means is called Jamming attacks. When it is done to target specific vital information is called selective jamming attack, various schemes are available to get rid of such attacks but somehow these measures become inefficient in uncertain situations. Recently 'Bazooka' the largest cyber attack till now hit the cyber world which resulted into crashing internet worldwide, it was like nuclear blast in cyber world. Bazooka is also an intentional inference attack. In present system Rate adaptation scheme is used to save messages and supports end to end delivery of message. Rate adaptation scheme is implemented by achieving high link utilization by adjusting mode of transmission according to expected maximum throughput. I have given detailed description of this scheme in my last paper. But I can say this scheme is not efficient to secure messages of high importance and also doesn't assures the uninterrupted service. So we have demonstrated few other schemes. Such as Dissembling commitment scheme and Puzzle dissembling scheme along with All Or Nothing Transformations.

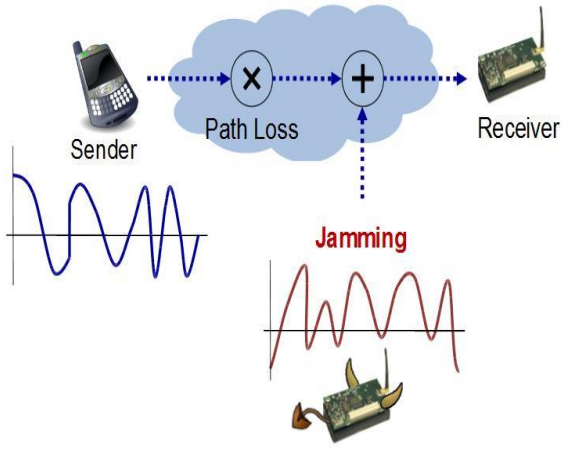

Figure 1: Jamming in wireless network

II. PROPOSED SYSTEM

Jamming can accomplished by the knowledge of Protocol specification and network secrets and in problem of selective jamming, attackers try to hit the system for short period of time and get the important messages.

To prevent or remove such attack we will focus on following schemes:

1) Combining the cryptographic primitives with physical layer attributes.
2) Analyse security
3) Evaluate computational & communicational overhead.

Security of important messages and jamming Prevention is accommodated by change in architecture of the existing system it means the previous architecture is considered to be less efficient for such purpose. Given below is proposed architecture, which starts with the source and after performing dissembling operations on the data to be secured it pass that data to the source and finally after application of decoding operations data is retrieved and saved from selective jamming.

Complete explanation in detail is given after figure.

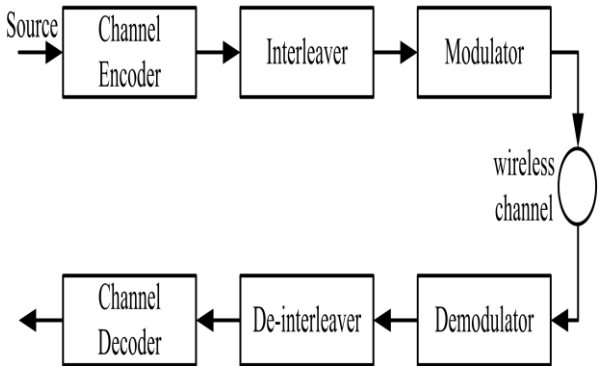

Figure 2: Proposed System Architecture

Original message is transformed first with the help of all or nothing transformation (AONT), which helps in reducing brute force attack, that is done by checking all the possible combination till the correct key is found and traversing the search space. Then it goes through channel encoder where binary conversion occurs and then few dissembling operations are performed into binary bits. Encoded Binary stream is passed through Interleaver which results in clubbing all odd and even input. Then analog signal taken from interleaver is passed through modulator for varying properties i.e. converting low frequency signals into R.F. signal.

(Low) (RF) (Can be transmitted)

Now the message is being transmitted to the wireless channel and jammer try to attack through route request/ route reply message or TCP acknowledgement. To get access of important message he must imply 'classy then jam' strategy. It means he must classify the transmitted packets using protocol knowledge and then he will decode the packet. But due to high security at physical layer he will not be able to decode before the packet reaches destination. Hence jam could not be accomplished and packet is demodulated then de-interleaved and decoded at destination to get its original form.

III. MODULE DESCRIPTION

A. Network module

The network consists of many nodes connected through wireless links. Nodes can communicate directly if they are in communication range, or indirect communication can also occur through multi hops. Nodes can communicate through both unicast and broadcast mode. Communication can be unencrypted or encrypted. For encrypted broadcast communications, symmetric keys are shared among all intended receivers. These keys are decided using asymmetric cryptography. We address the problem of avoiding the jamming from classifying message in real time, thus challenging and overcoming the jammers ability to perform jamming.

B. Packet Classification

Consider the communication system depicted in Architecture Fig. 2 At the physical layer, a packet is encoded through channel encoder, interleaved through interleaver, and modulated for varying properties through modulator before it floats over the wireless channel. At the receiver end, the signal is de-modulated, de-interleaved, and decoded, to recover the original message.

For our system only known people can classify packet through this type of encryption. Hence, attacker won't be able to access the important messages.

C. Dissembling commitment scheme (DCS)

Dissembling commitment scheme (DCS) is based on symmetric cryptography. Our main aim is to satisfy the strong concealing property and keeping the computation and communication overhead to a minimum.

The computation overhead of DCS is just a pair of symmetric encryption and decryption at sender and receiver ends. Because the header information is permuted as a trailer and encrypted, all receivers in the vicinity of a sender must receive the entire packet and decrypt it, before the packet type and destination can be determined However, in wireless protocols such as 802.11, the complete packet is received at the MAC layer before it is decided if the packet must be discarded or be further processed. If some parts of the MAC header are deemed not to be useful information to the jammer, they can remain unencrypted in the header of the packet, thus avoiding the decryption operation at the receiver.

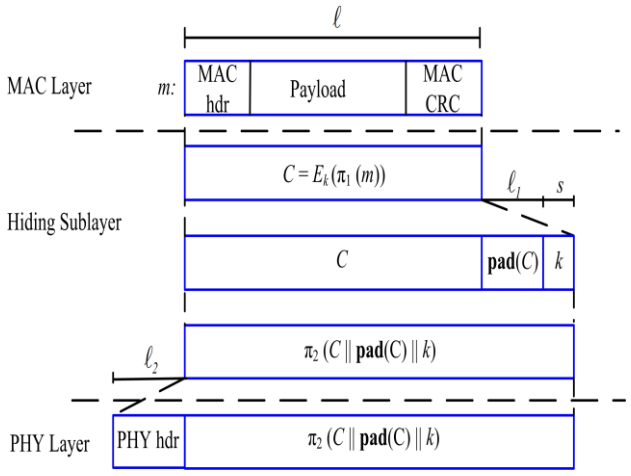

Figure 3: Dissembling Commitment Scheme

D. Puzzle dissembling scheme (PDS)

We present a packet hiding scheme based on cryptographic puzzles. The main idea behind such puzzles is to force the recipient of a puzzle execute a pre-defined set of computations before he is able to extract a secret of interest. The time required for obtaining the solution of a puzzle depends on its hardness and the computational ability of the solver. The advantage of the puzzle based scheme is that its security does not rely on the PHY layer parameters. However, it has higher computation and communication overhead

We consider several puzzle schemes as the basis for PDS. For each scheme, we analyze the implementation details which impact security and performance. Cryptographic puzzles 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.

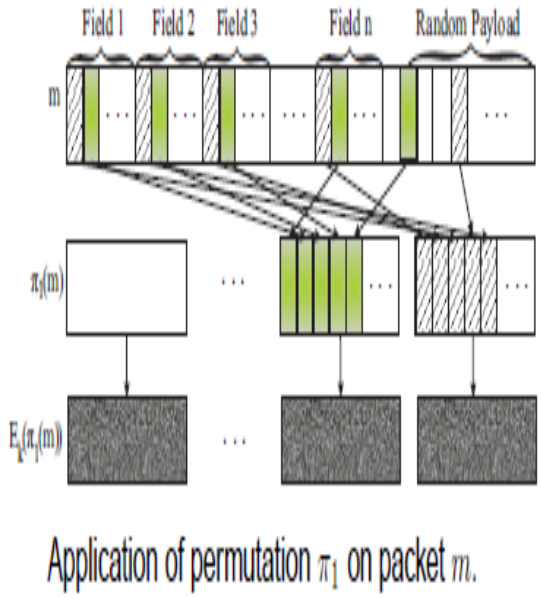

Figure 4: Puzzle Dissembling Scheme

E. AON TRANSFORMATION

Here AON stands for AON it means All or nothing, it means the receiver have to decode whole packet for retrieving the original message because if it receives half packet and it try to receive half message then that will be impossible for Jammer and jamming operation is also failed due to this scheme because jammer can never classify the data packet, which is most important for implement jamming.

IV. WIRELESS NETWORK DISCRIPTION

A. Sender node in wireless network:

Given Figure 5 shows the sender node which is blinking in green colour and all the other nodes are possible receivers.

Also sender is the starting component of wireless network from where the transmission begins.

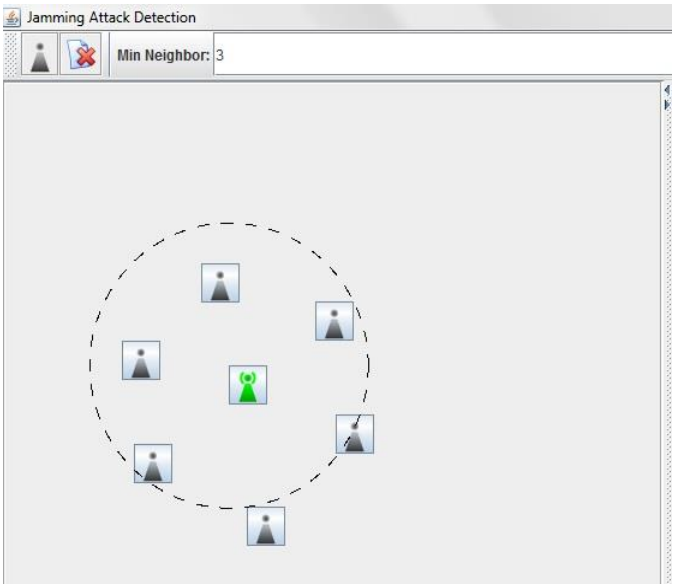

Figure 5: Receiver in WN

B. Receiver node in wireless network:

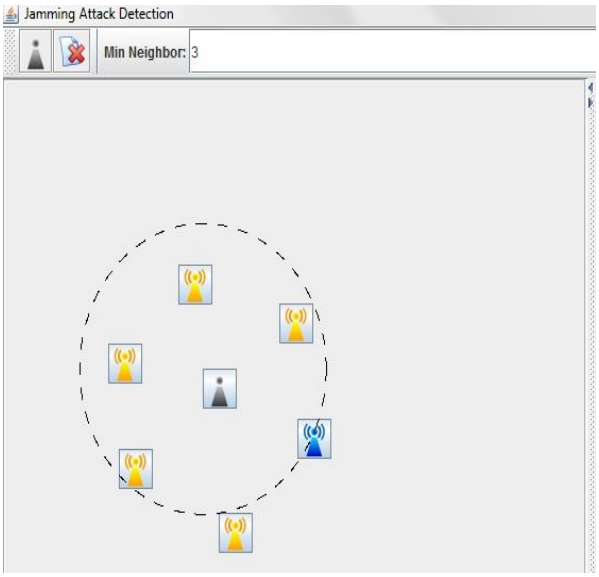

Figure 6: Receiver in WN

Node blinking in blue colour is receiver node and yellow ones are other nodes waiting for messages.

C. Jamming in wireless network:

This red symbol shows jamming in the sender nodes. As soon as this Red sign gets visible whole system interactions should stop and further processing occurs only when safe communication occurs.

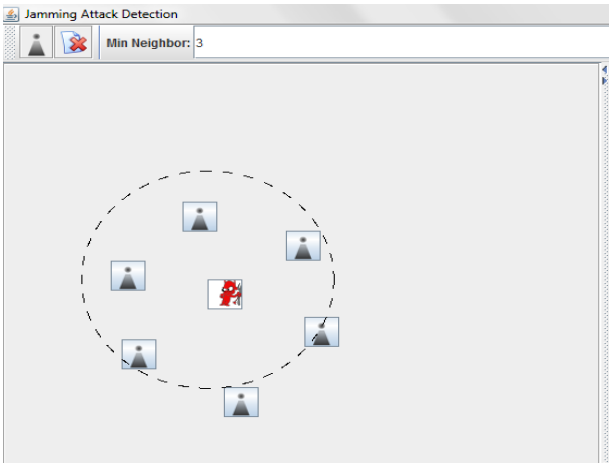

Figure 7: Jamming in WN

V. RESULT

A. *Channel encoding:*

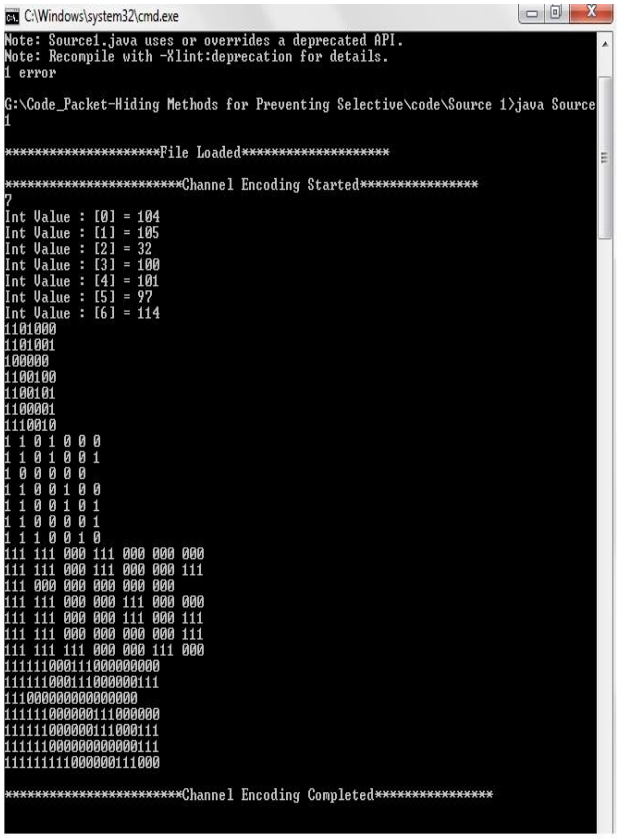

Figure: 8: Channel Encoding

Figure 8 shows how original message is being loaded and channel encoding is performed.

B. *Interleaving:*

After completion of channel encoding, file is interleaved which means all the even and odd bits are clubbed. Vice-versa process is used on receiver side to retrieve original message, which assure the secure and uninterrupted communication.

Figure 9: Interleaving

C. *Final Result*

Efficiency is given by efficiency of AONT because it is applied at the last layer of dissembling.

Efficiency: 99.59596
JBL: 21.0
Coding Rate: 0.666667
Interleaving Depth: 14.0
Formulations & calculations:
Since, File length: 7
Therefore, Jamming block length: 7*3 =21 (because each block is divided into 3 bits)
Also, Coding rate: Interleaving Depth / JBL
14/21= 0.666667

These all modules describe the wireless system and its components and uninterrupted communication with the selected important message security by dissembling through encoding and interleaving.

Figure 10: Final Result

VI. CONCLUSION

We addressed the problem of jamming in wireless networks and illustrated the effectiveness of jamming attacks, such as attacks against the TCP protocol. We showed that an adversary can exploit its knowledge of the protocol implementation to increase the impact of his attack at a significantly lower energy cost. We illustrated the feasibility of jamming attacks by performing real time packet classification. Showed PDS and DCS schemes through which the selective jamming can be prevented.

ACKNOWLEDGMENT

I would also like to express my sincere gratitude to all the faculties of ASET, Amity University for their extensive help and support during the writing this paper and continuously advising and guiding on the targets to be achieved for each week and evaluating the stages of experiments and suggestion improvements. But without their help, it would have been an extremely tedious task to come out with this research implementations and publications in such a limited span of time. I dedicate this paper to my family for their unconditional love and support in every way possible during the process of research and experimentations.

REFERENCES

[1] Stefania Sesia, Issam Toufik, and Matthew Baker, editors, LTE, The UMTS Long Term Evolution: From Theory to Practice, chapter 9. John Wiley & Sons Ltd, Chichester, West Sussex, United Kingdom, second edition, 2011.

[2] Mingyan Li, Iordanis Koutsopoulos and Radha Poovendran, Optimal Jamming Attacks and Network Defense Policies in Wireless Sensor Networks,infocom,2007

[3] Geethapriya Thamilarasu, Sumita Mishra and Ramalingam Sridhar, Improving Reliability of Jamming Attack Detection in Ad hoc Networks, International Journal of Communication Networks and Information Security (IJCNIS) Vol. 3, No. 1, April 2011

[4] Kwangsung Ju and Kwangsue Chung, Jamming Attack Detection and Rate Adaptation Scheme for IEEE 802.11 Multi-hop Tactical Networks, International Journal of Security and Its Applications Vol. 6, No. 2, April, 2012

[5] Alejandro Proa˜no and Loukas Lazos, Selective Jamming Attacks in Wireless Networks, Dept. of Electrical and Computer Engineering University of Arizona, Tucson, Arizona

[6] OPNETtm modeler 14.5. http://www.opnet.com/solutions/network rd/modeler.html.

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

[8] Shabnam Sodagari and T. Charles Clancy, Efficient Jamming Attacks on MIMO Channels, Bradley Dept of Electrical and Computer Engineering ,Virginia Tech, Arlington, VA,USA

[9] S. Jiang and Y. Xue (Eds.), Optimal Wireless Network Restoration under Jamming Attack, Proceedings of 18th International Conference on Computer Communications and Networks, (2009) August 3-9; Francisco, California.

[10] Tao Peng Christopher Leckie Kotagiri Ramamohanarao, Detecting Distributed Denial of Service Attacks Using Source IP Address Monitoring, ARC Special Research Center for Ultra-Broadband Information Networks.

[11] Pushphas Chaturvedi and Kunal Gupta, Detection and Prevention of various types of Jamming Attacks in Wireless Networks, IJCNWC,Vol 3, No 2, May 2013.

AUTHORS

First Author – Pushphas Chaturvedi, Pusuning M.Tech (CSE) from ASET, Amity University, Noida , India.
Pushphaschaturvedi@yahoo.com
Second Author – Kunal Gupta, Asst . Proffessor at ASET, Amity University, Noida , India.