REPORT OF RESEARCH PAPER

ON

A Review study on Jamming Attacks

Submitted to

LOVELY PROFESSIONAL UNIVERSITY

In partial fulfillment of the requirements for the award of degree of

Master in Computer Applications

Submitted By:

Mayank Bhandari

Reg.No:11401232

Supervised By:

Mr. Parvesh Mor

LOVELY FACULTY OF TECHNOLOGY AND SCIENCES

LOVELY PROFESSIONAL UNIVERSITY

PUNJAB

Index

Acknowledgement

I place my sincere thanks to my teacher Mr.Parvesh Mor for his supervision and advices to complete my work successfully. I also thank our HOD Mr.Balraj for providing me all the facilities to finish the term paper on time. My *RESEARCH PAPER* report on “Jamming Attacks” acknowledgement I would like to take this opportunity to express my gratitude towards all the people who have in various ways, helped in the successful completion of my term paper.

Introduction

Today, system security has become top priorities of all organization because if their system became victim of any type of attack then there is a risk to organization's data, network, etc. jamming attack in one of them. In jamming attack the jammer is an entity who is purposefully trying to interfere with the physical transmission and reception of wireless communications. Jammer continuously emits radio frequency signal to fill a blank wireless channel so that the legitimate channel will completely blocked. This attack has become the big problem for military because of radar and GPS jamming, the U.S. military put this jamming attack in its top threat. There are two types of radar jamming:

- **Mechanical jamming** is produced by those devices which reflect or re-reflect radar energy back to the radar by producing false target response on the operator's radar like: chaff, corner detector, decoys.
- **Electrical jamming** is a form of electronic warfare where the jammers radiate by interrupting the signals toward an enemy's radar, blocking the receiver with highly powered energy signals like: spot jamming, sweep jamming, cover pulse jamming, base jamming, pulse jamming, and deceptive jamming.

So, in this paper I will read the review of different papers and on the basis of them I will give the own methodology which describe how we can prevent jamming attack efficiently and also optimize the result in different types of jamming cases like: constant jamming, deceptive jamming, random jamming, reactive jamming.

Literature Review

Mithun Acharya *et.al.* had discussed about effect of jamming which require low power by using OPNET 11.5 & also showed types of jamming models as well as their impact on the networks.[1]

Table 1. Models of jammers

Model	**Description**
Constant jammer	Jammer continuously emits radio signal which force the device to do not wait for idle channel before transmitting.
Deceptive jammer	Jammer emits regular packets with no gap by which device in remain in receiving state & can't switch to the send state
Random jammer	It this there is alternate time between sleeping and jamming Sleeping period: jammer is inactive Jamming period: jammer is active.
Reactive jammer	This remains inactive until any activity on channel. It direct attacks on reception & hard to detect.

Kunal Gupta *et.al.* had discussed what is jamming attack and introduced efficient technique to conceal the important message.

Jamming attacks: In this attack a communication is intercepts by the device called jammer. By this attack the device loss their communication path by which many problem can occurs.[2]

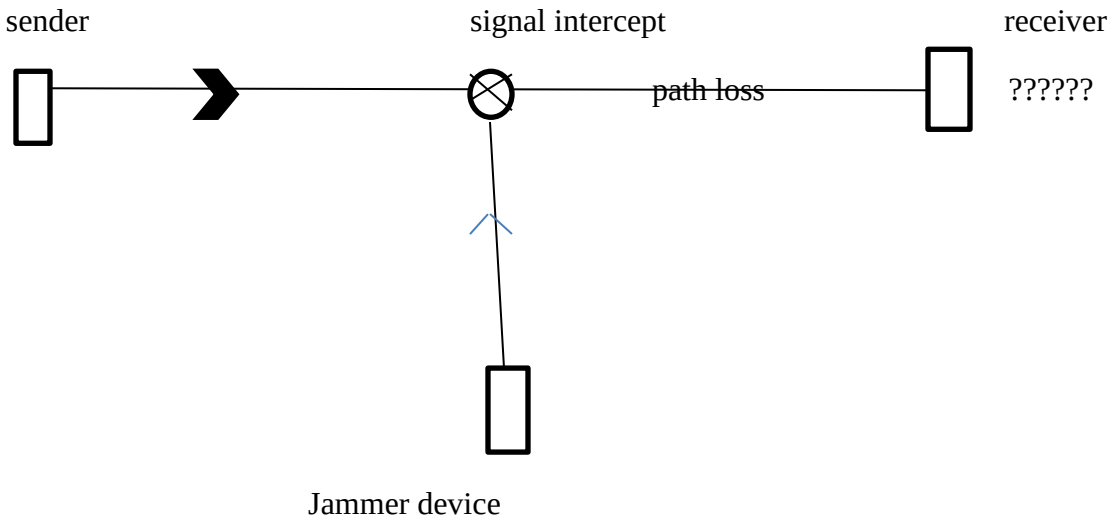

Fig.1 Jamming in wireless channel

Introduced technique:

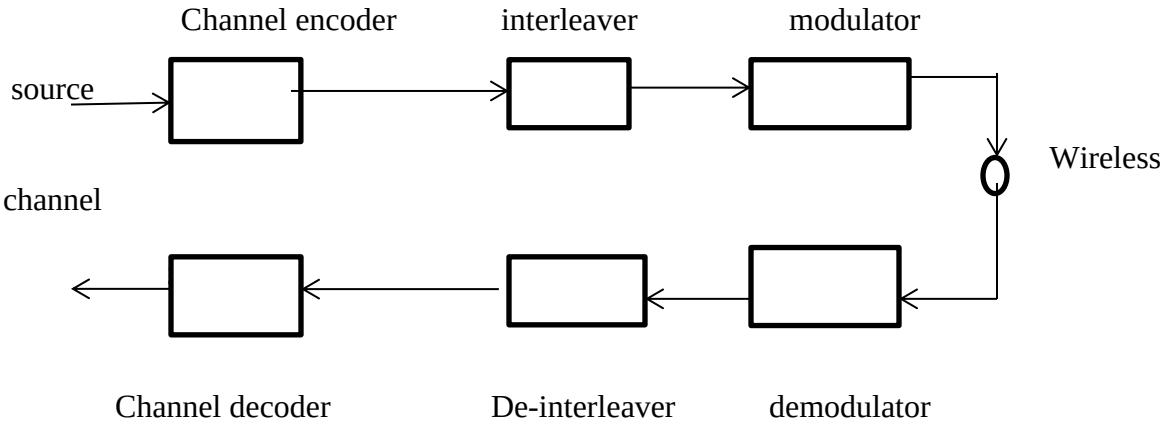

Fig2.Proposed technique architecture

In this original message is transforming with the help of ANOT (all or nothing transformation) which make use of make use of symmetric ciphers and may be applied before encryption. Then it transmits through channel encoder which converts into binary bits. Then it goes to interleaver which collects all types of input. Then signal pass to modulator which converts them into low frequency r.f signals. Then it enters through wireless channel & jammer will try to intercept the route reply message. The attackers classify the signal route then jam it because due to high security in physical layer intruder unable to decode the signal & message reach to the destination.

Y.E Sagduyu *et.al.* had discussed on possibility about jamming attacks failure due to empty packets queue into the transmitter & results that in jamming games. Jammer can't increase energy cost as well as can't decrease signals in transmitter.[3]

- **Random Access Game model with one transmitter & one jammer**:

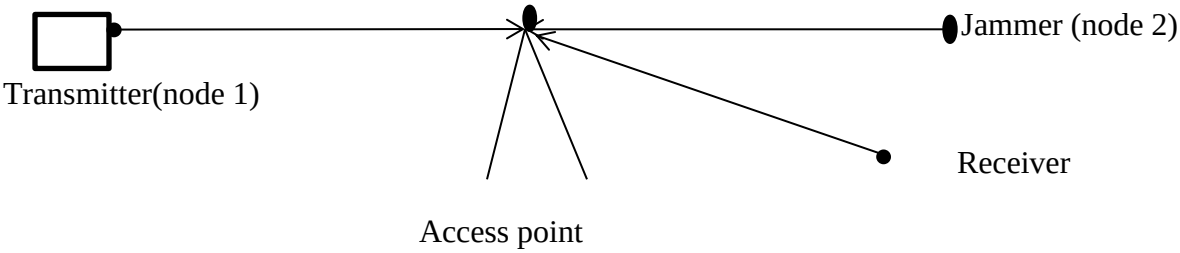

Fig.3 Single channel access point with one transmitter and one jammer

Considered that arrivals of packets are independent & it is difficult for jammer classify the transmission. So, non-cooperation game is introduced in which each node randomly transmit or wait in my time slot.

In the **Conclusion** there is comparison of two jammer attacks with & without queue & considered random state information & verified the low performance jammer if traffic of packet is random & queue state information is not available.

M.Li. *et.al.* had discussed scenario where intelligent jammer jams a single channel transmission and mentioned the various types of jamming cases ,also optimize among them which case creates the most negative impact on transmission channel.[4]

- Sensor network model:

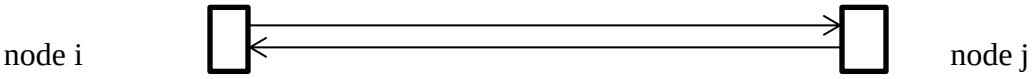

Fig.4 transmission of information from node i to node j

Assumed symmetric transmission in which node j can only receive signal from node (i) if node j is capable to send the signal to node i. Each node has its own fixed transmission power level with antenna and its transmission range and sensing range. A node which is in transmission range can decode message but node having sensing range can only see message in coded form if it has high signal strength. Transmission receives from node i can receive from its all neighborhood.

These all papers concluded that controllable jamming attacks are easy to attack and difficult to detect. Of particular interest of the comparison between the case of perfect knowledge in jamming and that if attacker has lack of knowledge then it can also jam the signals and the network about strategy of each other.

Table2. Comparison between paper 1 and paper 2

	Paper 1	Paper 2
Technique Introduced	• Proposed system architecture helps to reducing brute force attack in a different module description. (network module, packet classification, • Dissembling commitment scheme(DCS), Puzzle dissembling scheme(PDS)	• Solving optimization problem by constitute best responses of the attacker to the worst case strategy of each other. • By modeling different type of assumption in (sensor network model, attacker model, attack detection model)
Result	Showed feasibility of jamming attack by showing real time classification.	Optimize problems of optimal attack and network defense strategies

Table3. Comparison between paper 3 and paper 4

	Paper 3	Paper 4
Technology Introduced	Showed efficient jammer which use less energy cost and cannot decrease the feasible throughput for transmitters. By giving three cases. 1. No queue state information available at jammer. 2. Full queue state information available at jammer. Random errors in queue state information available at jammer.	Using Opnet 11.5 the effect of periodic jamming on throughput for an 802.11b network.
Result	• Observe jamming Games on the basis of MAC model. • Formulated non-cooperation jamming games in which the transmitter and jammer own choose the probability of collision channels.	Presented simulation results which show the effect of misbehaving node. Misbehaving nodes: (150bytes+28byte header)*200pkt/sec*8bits/pkt=284800bps.

Methodology

In this paper I'll propose a method which prevent a communication channel from jammer

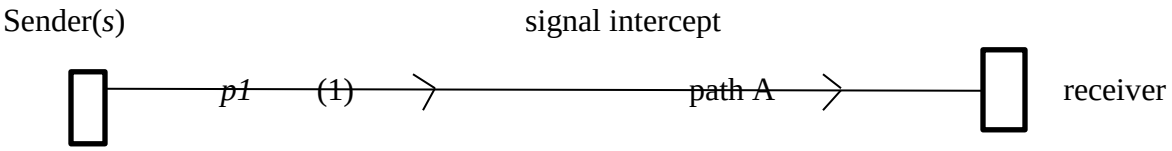

fig 4.simple circulation of information in a channel

In this figure the sender sending the information to the receiver through p1 path A and receiver can get the information whatever sender have sent without any interruption.

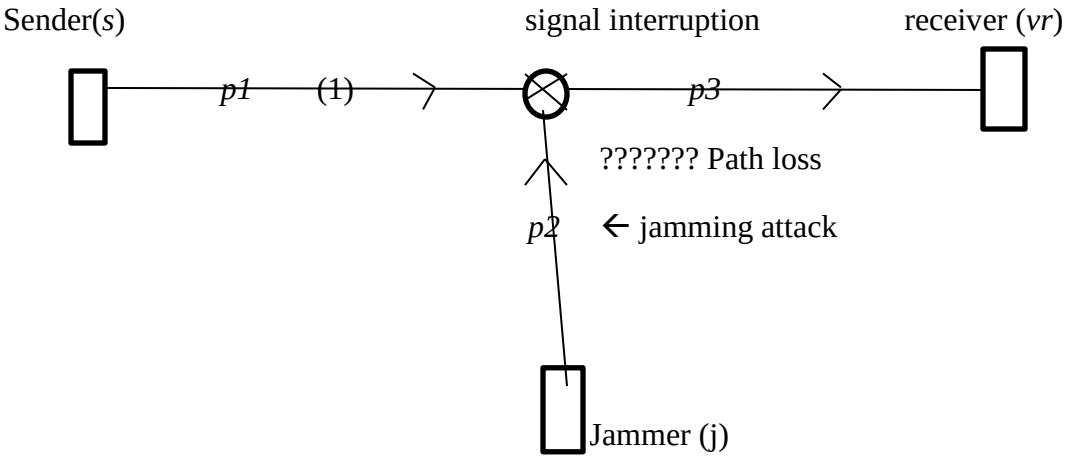

Fig.5 Jammer interrupting the communication channel

In this figure when the sender sends the information to the receiver the jammer (j) tries to jam the communication path between sender and receiver. By this, the signals have lost their path and receiver can't get proper information.

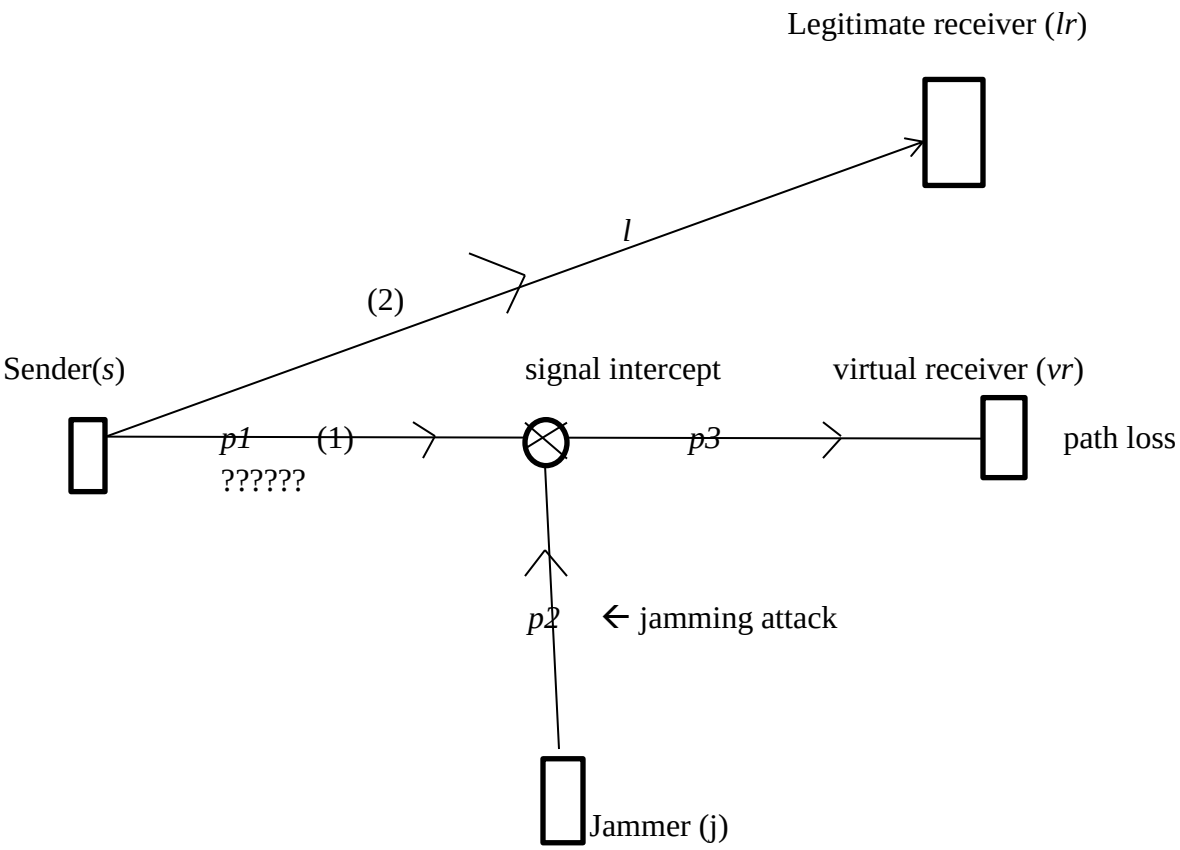

Fig 6.Prevention from jamming attack

Today, the jammer is very big problem mainly for the GPS satellites to interruption the signals. In 2012 N.Korea launched a series of jamming attacks against S.Korea which effect the navigation of ships and planes.

So, this methodology describes (In fig.6) how to prevent our communication from jamming attacks in various points:

- When the information will travel through path p1 then the jammer(j) will try to jam that communication line.
- But in this case there are two receivers one is legitimate (lr) and other is virtual (vr). When the signal emits the jammer jam that signal as shown in fig.6 but that information and receiver in not genuine.
- When the jammer busy to interrupt the signal then, again sender sends that information to that genuine receiver at random time of interval by which jam can't get idea of emission time.
- In this it is not mandatory that always first information goes first to the virtual receiver.

Conclusion

I studied the review of all papers and on the basis of them I gave the methodology to prevent any communication channel from jamming attack with the help of virtual receiver and generating a random timer which can send the information randomly. In further work I will implement this technique into communication system by taking three objects sender, receiver and jammer and optimize the result of prevention against different types of jamming attacks. This technique might be irresponsible in the case of constant jamming because in constant jamming the jammer continuously. It also can be irresponsible in some types of mechanical and electrical jamming of radar system.

References

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

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

[3] V. Gupta, S. V. Krishnamurthy, and M. Faloutsos, .Denial of Service Attacks at the MAC Layer in Wireless Ad Hoc Networks,. in Proc. IEEE Military Communications Conference, Anaheim, CA, Oct. 2002.

[4] T. S. Rappaport. *Wireless Communications: Principles and Practice*. Prentice Hall, 2 edition, 2001.