Hiding Methods for Preventing Jamming Attacks on Wireless Networks

J. Hirudhaya Mary Asha

Assistant Professor, Department of Computer science, GTN Arts College, Dindigul

Abstract- Wireless mediums open nature are capable for intentional interference attacks referred as jamming. This attacks paved a way for denial-of-service attacks on wireless networks. The intruder with immense knowledge of protocol specifications and network secrets can create low-effort jamming attacks that are difficult to detect and counter. In these attacks, the intruder is active only for a short period of time, selectively targeting messages of high importance. However, selective jamming attacks can be launched by performing real-time packet classification at the physical layer. To prevent these attacks, three schemes are developed to avoid real-time packet classification by combining cryptographic primitives with physical-layer attributes. Here, the security of the proposed methods is analyzed.

Index Terms- Selective Jamming , denial-of-service, wireless networks, packet classification

I. Introduction

Wireless networks rely on the uninterrupted availability of the wireless medium to interconnect participating nodes. However, its open nature vulnerable to multiple security threats. Anyone with a transceiver can eavesdrop on wireless transmissions, inject spurious messages or jam legitimate ones. while eavesdropping and message injection can be prevented using cryptographic methods, jamming attacks are harder to counter. They leads to severe denial-of-service (DoS) attacks against wireless networks [1], [5], [6], [7]. In the simplest form, the adversary interferes with the reception of messages by transmitting a continuous jamming signal [5] or several short jamming pulses [7].

The effects of jamming at the physical layer resonate through the protocol stack, providing an effective denial-of-service (DoS) attack on end-to-end data communication. The simplest methods to defend a network against jamming attacks comprise physical layer solutions such as spread-spectrum or beam forming, forcing the jammers to expend a greater resource to reach the same goal. However, intelligent jammers can incorporate cross layer protocol information into jamming attacks, reducing resource expenditure by several orders of magnitude by targeting certain link layer and MAC implementations as well as link layer error detection and correction protocols. The majority of anti-jamming techniques make use of diversity. For example, anti-jamming protocols may employ multiple frequency bands, different MAC channels, or multiple routing paths. Such diversity techniques help to curb the effects of the jamming attack by requiring the jammer to act on multiple resources simultaneously. Using multiple-path variants of source routing protocols such as Dynamic Source Routing (DSR) or Ad-Hoc On-Demand Distance Vector (AODV) , for example the MP-DSR protocol source node can request several routing paths to the destination node for concurrent use. To make effective use of this routing diversity, however, each source node must be able to make an intelligent allocation of traffic across the available paths while considering the potential effect of jamming on the resulting data throughput.

In order to capture the non-deterministic and dynamic effects of the jamming attack, model the packet error rate at each network node as a random process. At a given time, the randomness in the packet error rate is due to the uncertainty in the jamming parameters, while the time-variability in the packet error rate is due to the jamming dynamics and mobility. Since the effect of jamming at each node is probabilistic, the end-to-end throughput achieved by each source-destination pair will also be non-deterministic and, hence, must be studied using a stochastic framework. In this article, I thus investigate the ability of network nodes to characterize the jamming impact and the ability of multiple source nodes to compensate for jamming in the allocation of traffic across multiple routing paths. Our contributions to this problem are as follow: I formulate the problem of allocating traffic across multiple routing paths in the presence of jamming as a lossy network and formulate the centralized traffic allocation problem for multiple source nodes as a convex optimization

II. PROBLEM STATEMENT

Consider the scenario in fig.1(a) 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, J classifies m by receiving only few bytes of m. J then corrupts m beyond recover by interfering with its reception at B. we address the problem of preventing jamming node from classifying m in real time. Our goal is to transform a selective jammer to a random one.

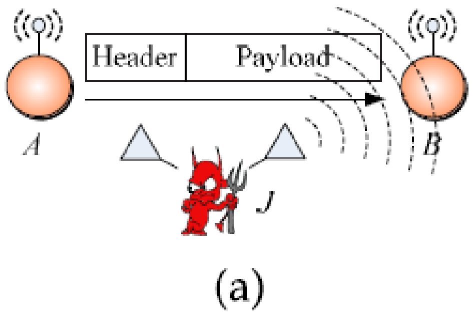


Fig.1(a) Realization of Selective Jamming attack

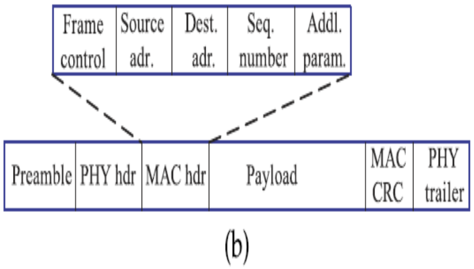


Fig.1(b) Generic frame format of a wireless network

1 Real-Time Packet Classification:

At the Physical layer, a packet m is encoded, interleaved, and modulated before it is transmitted over the wireless channel. At the receiver, the signal is demodulated, deinterleaved and decoded to recover the original packet m. 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.

2 A Strong Hiding Commitment Scheme

A strong hiding commitment scheme (SHCS), which is based on symmetric cryptography. Assume that the sender has a packet for Receiver. First, S constructs commit(message) the commitment function is an off-the-shelf symmetric encryption algorithm is a publicly known permutation, and k is a randomly selected key of some desired key length s (the length of k is a security parameter). Upon reception of d, any receiver R computes.

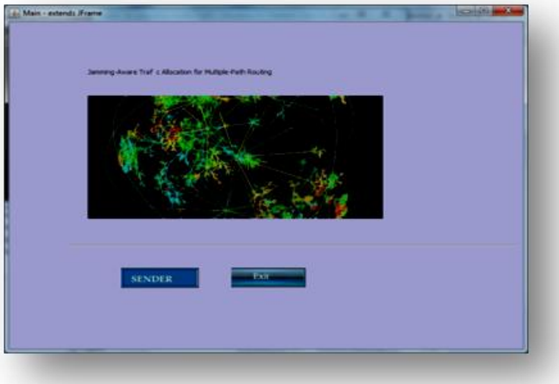
3 Cryptographic Puzzle Hiding Scheme

A sender S have a packet m for transmission. The sender selects a random key k , of a desired length. S generates a puzzle (key, time), where puzzle() denotes the puzzle generator function, and tp denotes the time required for the solution of the puzzle. Parameter 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). At the receiver side, any receiver R solves the received puzzle to recover key and then computes.

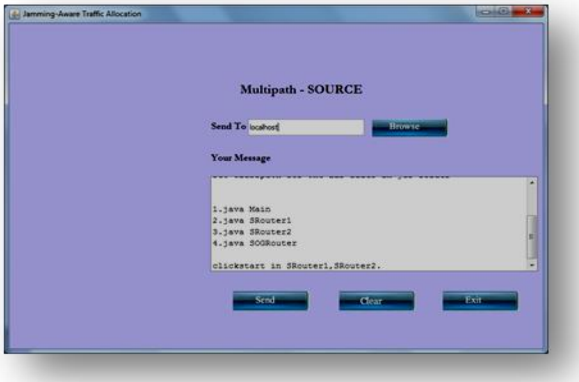
4 Hiding based on All-Or-Nothing Transformations

The packets are pre-processed by an AONT before transmission but remain unencrypted. The jammer cannot perform packet classification until all pseudo-messages corresponding to the original packet have been received and the inverse transformation has been applied.

III. EXPERIMENT RESULT -SCREEN SHOTS



This is the main page for the sender to send their message.



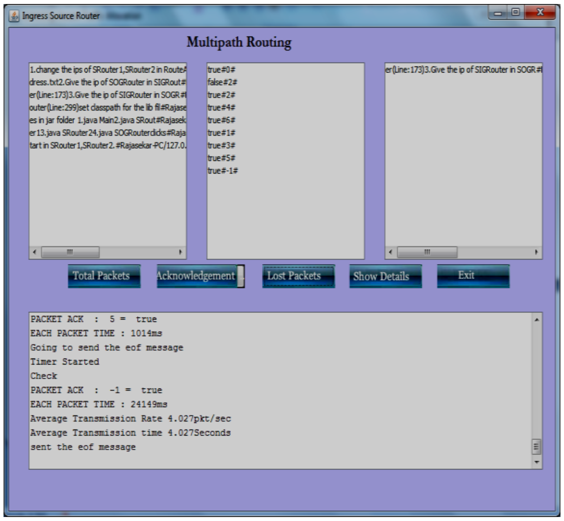
Send To localhost

Your Message

```
1.java Main
2.java SRouter1
3.java SRouter2
4.java SOGRouter

clickstart in SRouter1,SRouter2.
```

In the above screen illustrates the sender part, sender select the message to send to destination.



```
1.change the ips of SRouter1,SRouter2 in RouteA
dress.txt2.Give the ip of SOGRouter in SIGRout#
er(Line:173)3.Give the ip of SIGRouter in SOGR#
outer(Line:299)set classpath for the lib fil#Rajase
es in jar folder 1.java Main2.java SRout#Rajasek
er13.java SRouter24.java SOGRouterclicks#Raja
tart in SRouter1,SRouter2.#Rajasekar-PC/127.0.
```

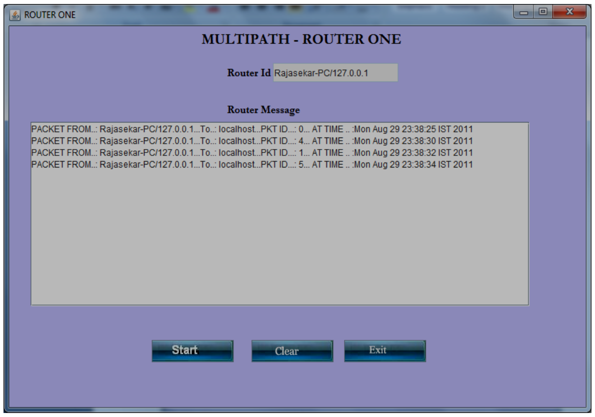
```
true#0#
false#2#
true#2#
true#4#
true#6#
true#1#
true#3#
true#5#
true#-1#
```

```
er(Line:173)3.Give the ip of SIGRouter in SOGR#
```

```
PACKET ACK  :  5 =  true
EACH PACKET TIME : 1014ms
Going to send the eof message
Timer Started
Check
PACKET ACK  :  -1 =  true
EACH PACKET TIME : 24149ms
Average Transmission Rate 4.027pkt/sec
Average Transmission time 4.027Seconds
sent the eof message
```

This shows the ingress router to receive all user data before it sends to jammer. If any packet losses is happen it will be view here itself.

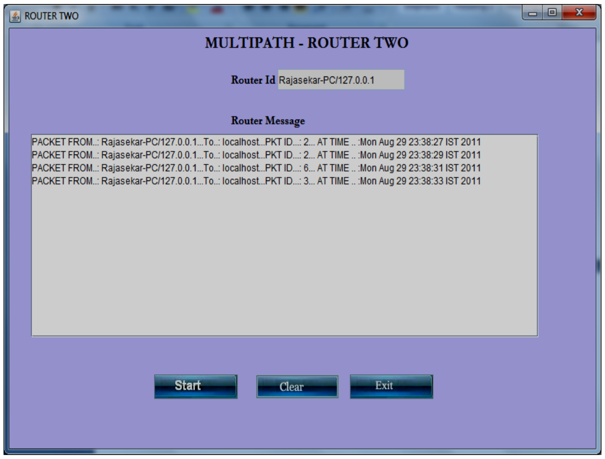
Routing-router one



Router Id: Rajasekar-PC/127.0.0.1

```
PACKET FROM..: Rajasekar-PC/127.0.0.1...To..: localhost...PKT ID...: 0... AT TIME .. :Mon Aug 29 23:38:25 IST 2011
PACKET FROM..: Rajasekar-PC/127.0.0.1...To..: localhost...PKT ID...: 4... AT TIME .. :Mon Aug 29 23:38:30 IST 2011
PACKET FROM..: Rajasekar-PC/127.0.0.1...To..: localhost...PKT ID...: 1... AT TIME .. :Mon Aug 29 23:38:32 IST 2011
PACKET FROM..: Rajasekar-PC/127.0.0.1...To..: localhost...PKT ID...: 5... AT TIME .. :Mon Aug 29 23:38:34 IST 2011
```

Router two

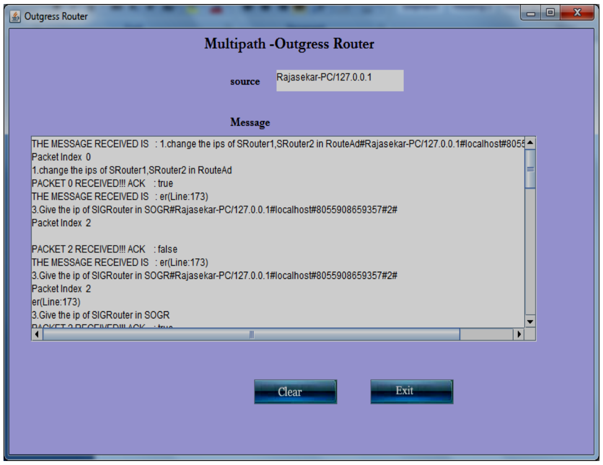


Router Id: Rajasekar-PC/127.0.0.1

```
PACKET FROM..: Rajasekar-PC/127.0.0.1...To..: localhost...PKT ID...: 2... AT TIME .. :Mon Aug 29 23:38:27 IST 2011
PACKET FROM..: Rajasekar-PC/127.0.0.1...To..: localhost...PKT ID...: 2... AT TIME .. :Mon Aug 29 23:38:29 IST 2011
PACKET FROM..: Rajasekar-PC/127.0.0.1...To..: localhost...PKT ID...: 6... AT TIME .. :Mon Aug 29 23:38:31 IST 2011
PACKET FROM..: Rajasekar-PC/127.0.0.1...To..: localhost...PKT ID...: 3... AT TIME .. :Mon Aug 29 23:38:33 IST 2011
```

In this screen is the Receiver or Router two that is available node in the network.

Receiver

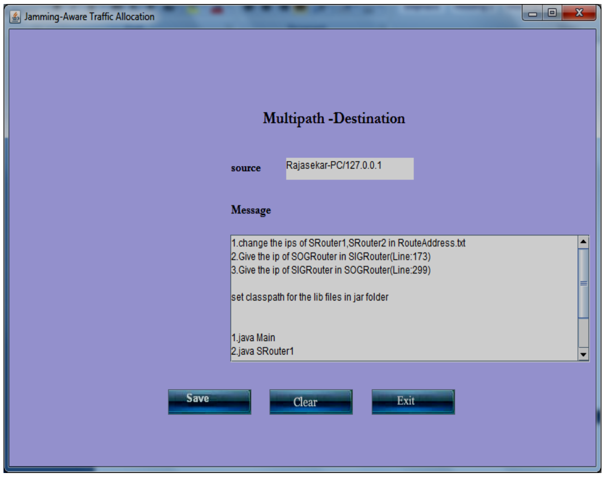


source: Rajasekar-PC/127.0.0.1

```
THE MESSAGE RECEIVED IS   : 1.change the ips of SRouter1,SRouter2 in RouteAd#Rajasekar-PC/127.0.0.1#localhost#8055
Packet Index  0
1.change the ips of SRouter1,SRouter2 in RouteAd
PACKET 0 RECEIVED!!! ACK   : true
THE MESSAGE RECEIVED IS   : er(Line:173)
3.Give the ip of SIGRouter in SOGR#Rajasekar-PC/127.0.0.1#localhost#805590865935 7#2#
Packet Index  2

PACKET 2 RECEIVED!!! ACK   : false
THE MESSAGE RECEIVED IS   : er(Line:173)
3.Give the ip of SIGRouter in SOGR#Rajasekar-PC/127.0.0.1#localhost#8055908659357#2#
Packet Index  2
er(Line:173)
3.Give the ip of SIGRouter in SOGR
PACKET 2 RECEIVED!!! ACK   : true
```

Outgress router get data from the connected node in the networks



source: Rajasekar-PC/127.0.0.1

```
1.change the ips of SRouter1,SRouter2 in RouteAddress.txt
2.Give the ip of SOGRouter in SIGRouter(Line:173)
3.Give the ip of SIGRouter in SOGRouter(Line:299)

set classpath for the lib files in jar folder


1.java Main
2.java SRouter1
```

Receiver can receive the data from sender through in which the outgress router. The outgress router directly connected with receiver.

IV. CONCLUSION

The problem of traffic allocation in multiple-path routing algorithms in the presence of jammers whose effect can only be characterized statistically for each network node to probabilistically characterize the local impact of a dynamic jamming attack and for data sources to incorporate this information into the routing algorithm. I formulated multiple-path traffic allocation in multi-source networks as a lossy network flow optimization problem using an objective function based on portfolio selection theory from finance. I showed that this centralized optimization problem can be solved using a distributed algorithm based on decomposition in network utility maximization (NUM) presented simulation results to illustrate the impact of jamming dynamics and mobility on network throughput. I have thus shown that multiple path source routing algorithms can optimize the throughput performance by effectively incorporating the empirical jamming impact into the allocation of traffic to the set of paths**.**

FUTURE ENHANCEMENT

I developed Jamming Aware Traffic allocation ,but lack of packet retransmitting while packets getting jamming ,so I extended this model with packet retransmitting.

REFERENCES

[1] T.X. Brown, J.E. James, and A. Sethi, “Jamming and Sensing of Encrypted Wireless Ad Hoc Networks,” Proc. ACM Int’l Symp. Mobile Ad Hoc Networking and Computing (MobiHoc), pp. 120-130,2006.

[2] M. Cagalj, S. Capkun, and J.-P. Hubaux, “Wormhole-Based Anti-Jamming Techniques in Sensor Networks,” IEEE Trans. MobileComputing, vol. 6, no. 1, pp. 100-114, Jan. 2007.

[3] A. Chan, X. Liu, G. Noubir, and B. Thapa, “Control Channel Jamming: Resilience and Identification of Traitors,” Proc. IEEE Int’l Symp. Information Theory (ISIT), 2007.

[4] T. Dempsey, G. Sahin, Y. Morton, and C. Hopper, “IntelligentSensing and Classification in Ad Hoc Networks: A Case Study,” IEEE Aerospace and Electronic Systems Magazine, vol. 24, no. 8 pp. 23-30, Aug. 2009.

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

[6] K. Gaj and P. Chodowiec, "FPGA and ASIC Implementations of AES," Cryptographic Engineering, pp. 235-294, Springer, 2009.

[7] O. Goldreich, Foundations of Cryptography: Basic Applications. Cambridge Univ. Press, 2004.

[8] B. Greenstein, D. Mccoy, J. Pang, T. Kohno, S. Seshan, and D. Wetherall, "Improving Wireless Privacy with an Identifier-Free Link Layer Protocol," Proc. Int'l Conf. Mobile Systems, Applications, and Services (MobiSys), 2008.IEEE, IEEE 802.11 Standard, http://standards.ieee.org/getieee802/download/802.11-2007.pdf, 2007.Juels and J. Brainard, "Client Puzzles: A Cryptographic Countermeasure against Connection Depletion Attacks," Proc.

[9] Network and Distributed System Security Symp. (NDSS), pp. 151-165,1999.

AUTHORS

First Author –J.Hirudhaya Mary Asha, Assistant Professor., Department of Computer Science, GTN Arts College, Dindigul, hirudhaya_ashaa20@yahoo.co.in