International Journal of Electrical and Electronics Engineers
Vol. No.7 Issue 02, July-December 2015
www.arresearchpublication.com
IJEEE
ISSN 2321 - 2055

ANALYSIS OF METHODS FOR PREVENTING SELECTIVE JAMMING ATTACKS USING NS-2

Mr.Ganesh R.Patil[1], Prof. Prashant S.Wankhade[2]

[1]*PG Scholar,Dept of Electronics &Telecomm. Engg, ARMIET, Asangaon, Mumbai (India)*

[2]*Assistant Professor, Dept of Electronics Engg, Datta Meghe College of Engineering, Airoli, Navi Mumbai, (India)*

ABSTRACT*:*

The wireless networks are more sensitive to the Denial-of-Service (DoS) attacks. The existing system is based on Spread Spectrum (SS). This technique mainly focuses on an external threat model. In wireless network the communications between nodes take place through broadcast communication. That is why, if an attacker present within the network can easily eavesdrop the message sent by any node. The performance of the proposed scheme is to be evaluated through a series of simulations with the ns-2 network simulator.

Keywords: WSN,NAM file,TCL file,NS2simulator.

I. INTRODUCTION

The network consists of a collection of nodes connected via wireless links. Nodes may communicate directly if they are within communication range, or indirectly multiple hopes. Nodes communicate both in unicast mode and broadcast mode. Communication can be either unencrypted or encrypted. For encrypted broadcast communications, sysmetric krys are shred among all intended receivers. These keys are established using preshared pairwise keys or asymmetric cryptography. Conventional anti-jamming techniques rely extensively on spread-spectrum (SS) communications or some form of jamming evasion (e.g., slow frequency hopping, or spatial retreats). SS techniques provide bit-level protection by spreading bits according to a secret pseudo-noise (PN) code, known only to the communicating parties. These methods can only protect wireless transmissions under the external threat model.

We illustrate the impact of selective jamming attacks on the network performance. We used OPNET Modeler 14.5 to implement selective jamming attacks in two multihop wireless network scenarios. In the first scenario, the attacker targeted a TCP connection established over a multihop wireless route. In the second scenario, the jammer targeted network-layer control messages trans- mitted during the route establishment process.

1.1 .Selective Jamming at the Transport Layer

In the first set of experiments, we set up a file transfer of a 3 MB file between two users A and B connected via a multihop route. The TCP protocol was used to reliably transport the requested file. At the MAC layer, the RTS/ CTS mechanism was enabled. The transmission rate was set to 11 Mbps at each link. The jammer was placed within the proximity of one of the intermediate hops of the TCP connection. Four jamming strategies were considered:

1.Selective jamming of cumulative TCP-ACKs.

2.Selective jamming of RTS/CTS messages.

3.Selective jamming of data packets.

4.Random jamming of any packet.

1.2 Selective Jamming at the Network Layer

In this scenario, we simulated a multihop wireless network of 35 nodes, randomly placed within a square area. The AODV routing protocol was used to discover and establish routing paths. Connection requests were initiated between random source/destination pairs. Three jammers were strategically placed to selectively jam no overlapping areas of the network. Three types of jamming strategies were considered:

1) a continuous jammer.

2) a random jammer blocking only a fraction p of the transmitted packets.

3) a selective jammer targeting route-request (RREQ) packets**.**

II. GENERATION OF TCL AND NAM FILES

2.1 TCL Script (run.tcl)

TCL Script **(run.tcl)** which we are using defines all nodes and all required parameters.

```
Set nn                                  # number of mobile nodes
set ns [new simulator]                  #simulator object creation
set f [open Trace.tr w]                 #trace file to record all the events
set namtrace[openNam . nam w]           #NAM window creation
set topo[new Topology]                  #topology creation
set god_[create-god $ nn]               #node creation
proc weight {}                          #set color,create des x  y file
proc source {}                          #---source---
proc destination {}                     #---destination---
proc finish{}                           #finish procedure to exec NAM window
```

2.2 NAM File Network Animator File (Nam.nam)

When a simulation is finished, NS produces one or more text-based output files that contain detailed simulation data, i.e **Nam.nam** if specified to do so in the input Tcl (or more specifically, Otcl) script. The data can be used for simulation analysis (two simulation result analysis examples are presented in later sections) or as an input to a graphical simulation display tool called Network Animator (NAM). NAM has a nice graphical user interface similar to that of a CD player (play, fast forward, rewind, pause and so on), and also has a display speed controller. Furthermore, it can graphically present information such as throughput and number of packet drops at each link, although the graphical information cannot be used for accurate simulation analysis.

III. RESULT

We use the NS-2 simulator for examining our desired results we get following output.

Step 1. – After run the TCL script **(run.tcl)** in terminal by command we get fig 1.

Step 2.- Secondly execute **Nam.nam** NAM file NAM file (Network Animator File) we get fig 2 .

Step 3. – Finally after completion the Simulation with desired time the file is generated and result shown below

In fig.3.

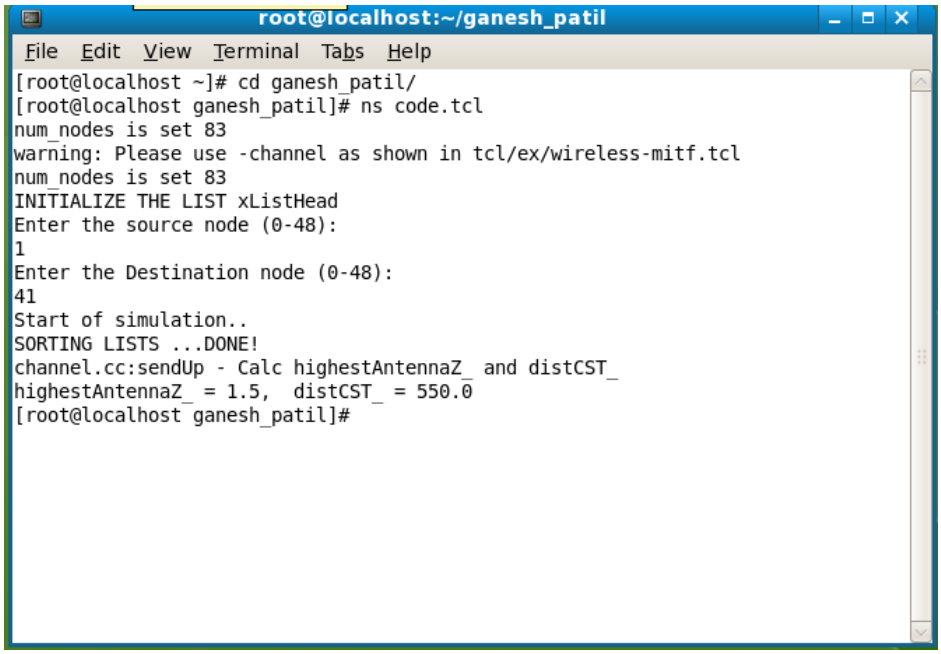

Fig 1. Step 1 Result

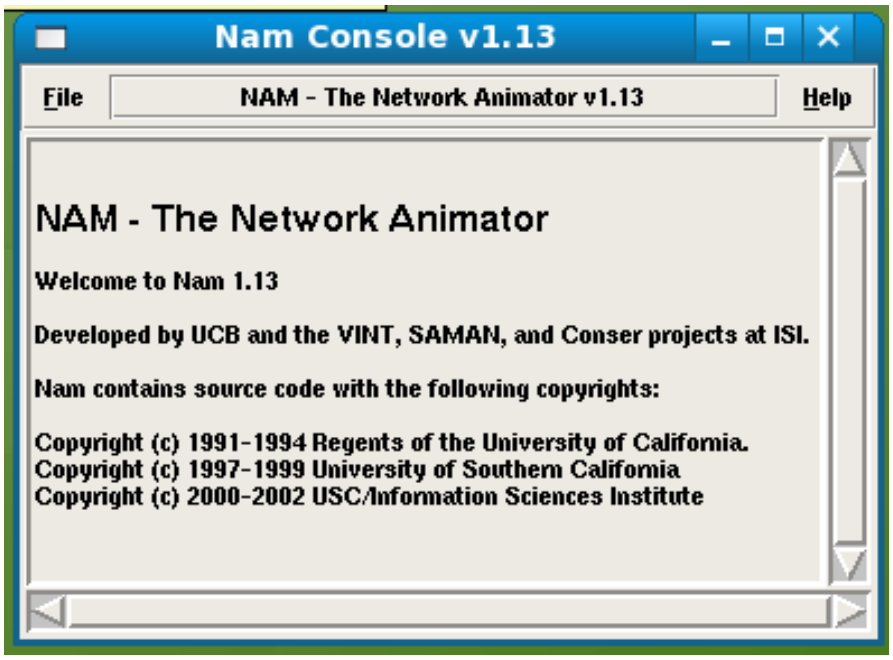

Fig 2. Step 2 Result

International Journal of Electrical and Electronics Engineers
Vol. No.7 Issue 02, July-December 2015
www.arresearchpublication.com
IJEEE
ISSN 2321 - 2055

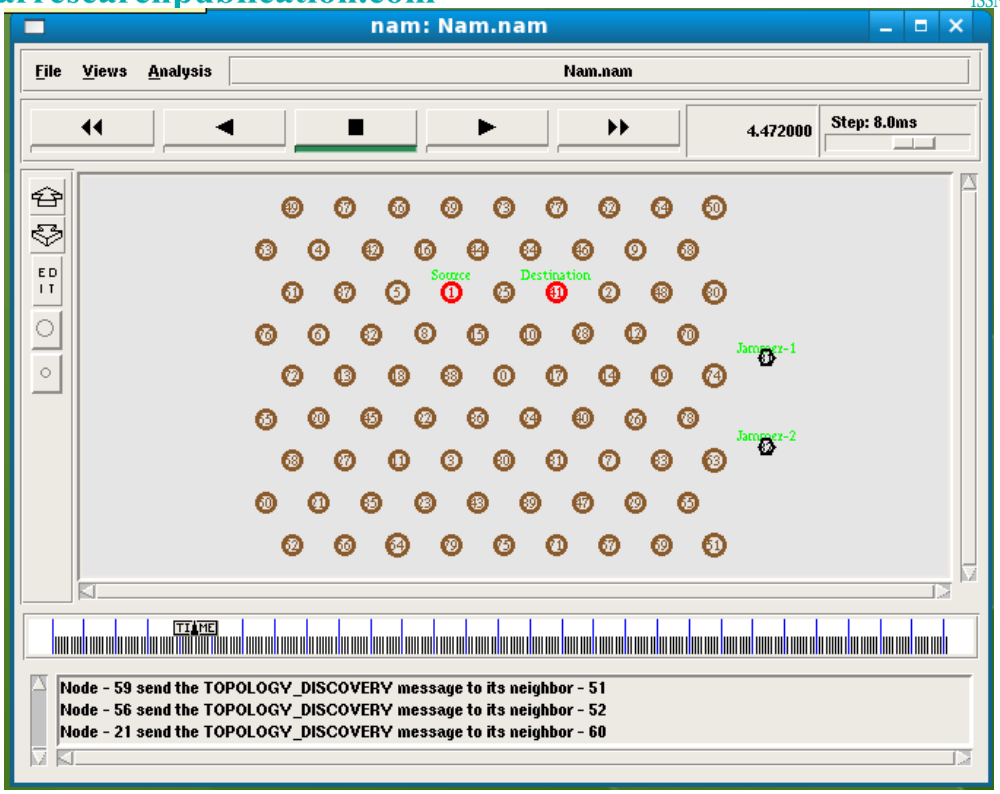

Fig 3. Step 2 Result

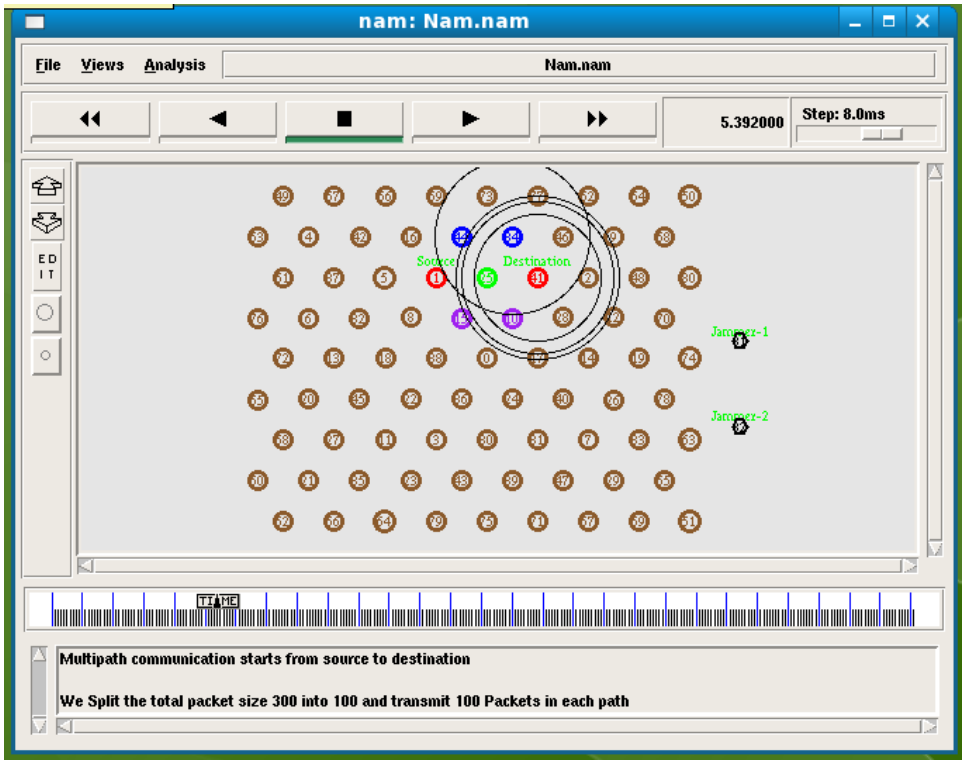

Fig 4. Step 2 Result

International Journal of Electrical and Electronics Engineers
Vol. No.7 Issue 02, July-December 2015
www.arresearchpublication.com
IJEEE
ISSN 2321 - 2055

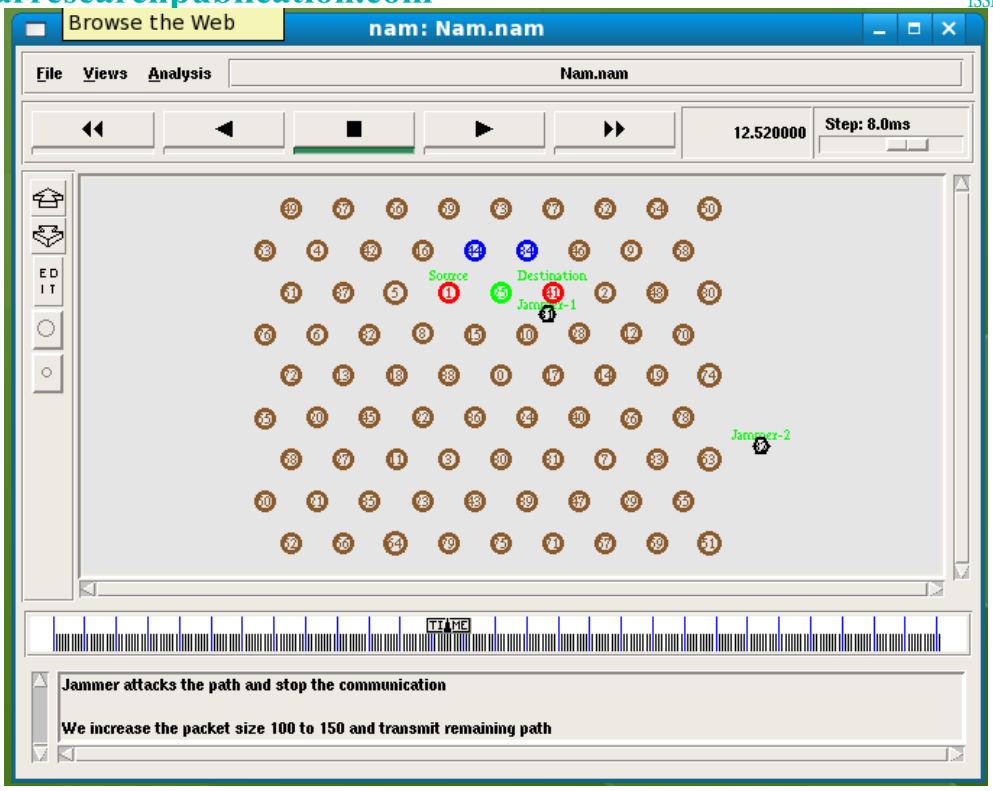

Fig 5. Step 3 Result

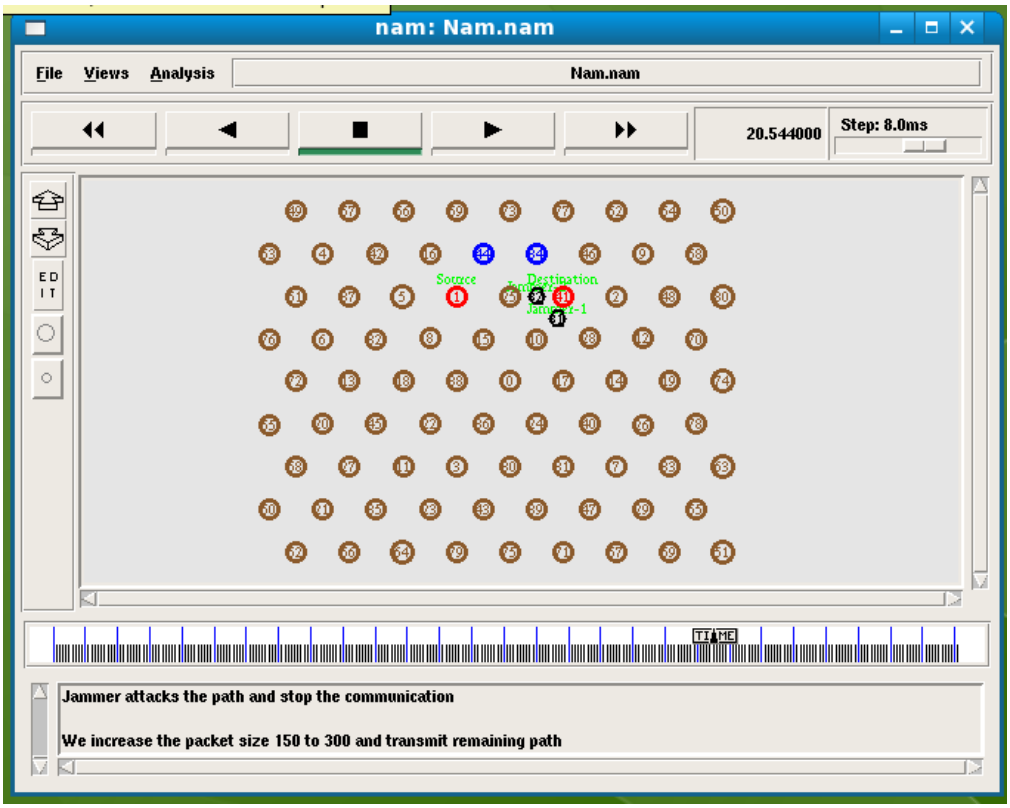

Fig 6. Step 3 Result

IV. CONCLUSION

After simulating the source and destination formation file on Network Simulator (version 2.32) widely known as NS2, a scalable discrete-event driven simulation tool.

Building high performance WSN network systems requires an understanding of the behavior of sensor network and what makes them fast or slow. In addition to the performance analysis, we have also evaluated the proposed technique in measuring, evaluating, and understanding system performance. The final but most important step in our experiment is to analyze the output from the simulation. After the simulation we obtain animation which shows the movement of nodes along with the snake type dynamic movement and various node points. With the help of that we will identify the location of all nodes finally the location details file generated which contains the Source, Destination, SX-Pos, SY-Pos, Distance(d) .

Thus we conclude that the different methods of selective jamming attacks at source and destination nodes were studied and verified the desired output.

REFERENCES

[1] Alejandro Proan˜o and Loukas Lazos, "Packet-Hiding Methods for Preventing Selective Jamming Attacks" Ieee Transactions On Dependable And Secure Computing, Vol. 9, No. 1, January/February 2012.

[2] R.C. Merkle, "Secure Communications over Insecure Channels,"Comm. ACM, vol. 21, no. 4, pp. 294-299, 1978.

[3] T. Dempsey, G. Sahin, Y. Morton, and C. Hopper, "Intelligent B. Thapa, G. Noubir, R. Rajaramanand, and B. Sheng, "On theSensing and Classification in Ad Hoc Networks: A Case Study,"IEEE Aerospace andElectronic Systems Magazine, vol. 24, no. 8, pp. 23-30, Aug. 2009.

[4] Robustness of IEEE802.11 Rate Adaptation Algorithms against Smart Jamming," Proc. ACM Conf. Wireless Network Security (WiSec), 2011.

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

[6] M. Wilhelm, I. Martinovic, J. Schmitt, and V. Lenders, "Reactive Jamming in Wireless Networks: How Realistic Is the Threat," Proc. ACM Conf. Wireless Network Security (WiSec), 2011.

[7] W. Xu, W. Trappe, Y. Zhang, and T. Wood, "The Feasibility of Launching and Detecting Jamming Attacks in Wireless Net- works," Proc. ACM Int'l Symp. Mobile Ad Hoc Networking and Computing (MobiHoc), pp. 46-57, 2005.