USE OF JAMMER NETWORK TO DETECT DENIAL OF SERVICES ATTACK IN WIRELESS NETWORK

P.MOHANRAJ, A.MUMMOORTHY

[1] Master of Computer Science and Engineering ,K.S.R. College of EngineeringTiruchengode, India
[2]Assisant Professor, Department of CSE,K.S.R. College of Engineering, Tiruchengode, India

ABSTRACT:

The most important aspect of network is to share the data from one to another. It can either wired or wireless. Both networks provides similar kind of security only. The internet users can have experience of denial of services attack for hacking the data, to avoid the such a hacking provides many techniques to resolve the problem. The jammer is an electronic device used to distrupt the communication. The jammer is made of large number of tiny low power distributed jammer. Use of jammer to avoid the hacking of data. In a network the node setup purpose uses they percolation concept. Based on the network, jammer, performance are evaluated. Finally provides the results in simulation tool such as NS2.

KEY WORDS:

Network, Distrupt, DoS, Jammer, Percolation

1. INTRODUCTION

The wireless network can transfer the data threw the access point. The access point need not reach all the nodes in the network.

FIG.1: Wireless network components

1.1 Security in Wireless Network

A.Confidentiality
B.Integrity
C. Availability

1.2Denial of services attack

It is very common attack to wireless network. It may slow down or totally interrupt the service of a system.

1.2 Distributed jammer network (DJN)

Jammer is an electronic device used to disrupt the communication.Jammers are used by military and civilian applications because DJN can be deployed to form a low power (possibly air-born) jamming dust to disrupt the communication.

1.3.1 Advantage of DJN

A. Robust
B.Low power

1.3.2 Types of jammer

A.Constant jammer
B. Deceptive jammer
C. Random jammer

2. PHASE TRANSITION USING PERCOLATION THEORY

We consider a random connection model where each pair of points*(xi, xj)* of a Poisson point process of density λ is connected with probability *g(xi −xj)*, for some given function *g* :R2→[0, 1]. All connections areindependent of each other.

It is well knownfor g that for any function *g, H* there is a critical value $\lambda c(g)$ that ensures connectivity almost surely (a.s.), i.e., with probability one. This is defined as $0<\lambda c(g)=\inf\{\lambda : \exists$ infinite connected component a.s.$\}<\infty$.

When $\lambda > \lambda c$ we say that the random connection model *percolates*.The value of g(x) is 0 means the nodes are said to be inside the network, if the value is 1 means the nodes are said to be outside. To make inside the following two transformation methods used.

2.1 Squishing and Squashing Transformation

In this transformation technique used to transfer the data from one to another. Uses some mathematical notations. G and H are they two functions have the probability value of (0,1). The value is 0 means ready to transform if the value is 1make the adjustment to transform from one to another.

2.2 Shifting and Squeezing Transformation

We call this transformation g*s*hift*s (x)*. Here we "shift" the function *g*outwards distance *s*,but squeeze the function after that, so that it has the same effective area.

3. JAMMER EFFECTIVENESS

There are two metrics used to measure the effectiveness of a jammer that is PSR and PDR. In PDR the ratio of packet that are successfully delivered to a destination compared with number of packets send by the source. In PSR the sender can the data threw the receiver successfully.

3.1 Detecting jamming attacks

Three ways to detect them jamming attacks signal strength, carrier sensing time(CST) and PDR. In signal strength uses two approaches.In CST node A senes the channel by trying to send out a beacon to the node B. It obtain the channel sensing time D by calculating the difference between the time when beacon packets reach the destination sucessfully. In PDR has to be done in two ways sender site or receiver site. In sender site the PDR can be calculated by keeping track of how many acknowledgement it receiver from the receiver. In receiver site the PDR can be calculated using the ratio of the number of packets the CRC with respect to the number of packets received.

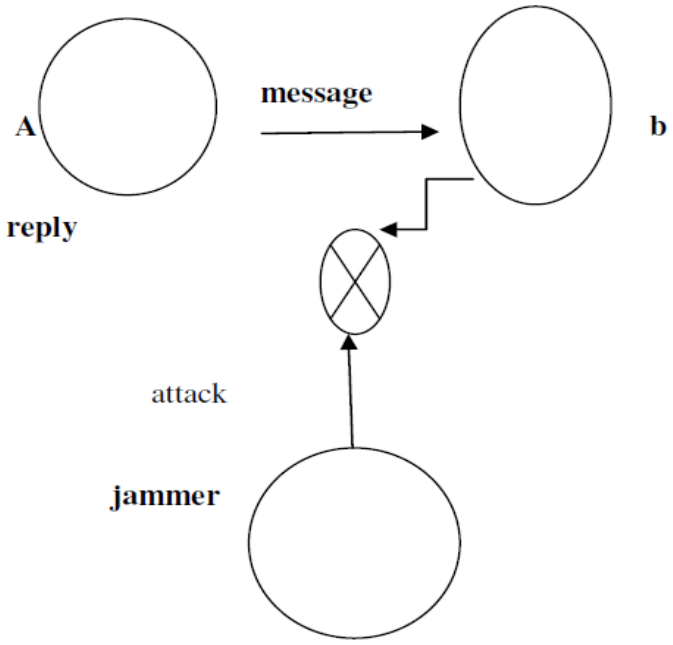


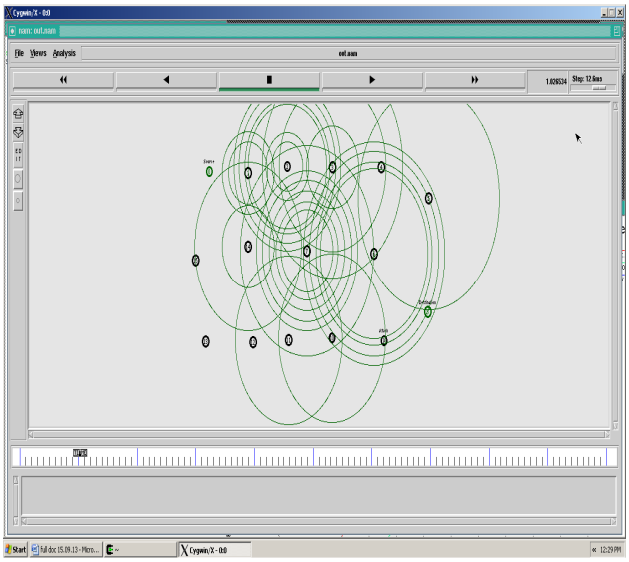
FIG 2. Over All System Architecture

4. RELATED WORK

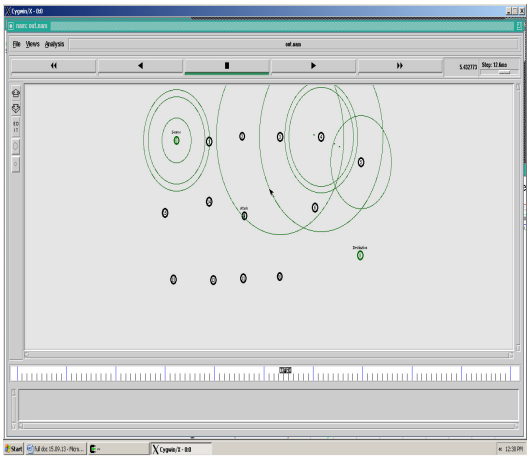
Jamming assault on wireless networks was usually treated from the viewpoint of human being jammers. We advocate a move toward based on the network viewpoint, and using this networked approach we show that some attractive results can be obtained. We used show that DJN can cause a stage transition in the presentation of the objective network. We employ percolation assumption to explain such phase change, to analyze the impact of DJN on the connectivity of the target network, and to give lower and upper bounds for the percolation of the objective network to come about in the presence of DJN. To providing a large scaling examination of the jamming in relation to the jammer node with density, we present simulation results recitation the impact of DJN topology on the jamming efficiency**.** In proposed system to demonstrated that DJN can

cause a phase change in target network presentation even when the total overcrowding power is held stable. We explained the stage changeover using percolation theory, analyzed scaling performance of node thickness and numeral of nodes in DJN, and we also investigate the impact of DJN topology on the overcrowding effectiveness. We believe awaiting the problem of jamming in wireless networks from a set of connections perspective can broaden the investigate scope significantly and can bring out some motivating results otherwise unachievable by focusing on person jammers. Also using we think the interaction between DJN and DWN makes for intriguing problems, which cut across system layers: device assignment, topology control, authority control, medium access, routing, and data transport. Investigating those troubles can result in deeper sympathetic of not only DJN but DWN as well. We believe a group more interesting consequences can be obtain from this move toward and are currently operational in this course.

4.1 Result analysis



In this figure the nodes are created with different distance. It also sets the attacker and source, destination.



The attacker can hack the information. After hacking the information the source can choose the other path to receive the destination. The jammers aretaken the authenticated data.

5. CONCLUSION

The Reactive Defence Mechanism it's used to moderate the DDoS attack and additional get better system presentation in conditions of a smaller amount working out time. Supplementary the reproduction product proves it to be an enhanced result leaning approach. Secondly we need a systematic procedure for setting the parameters according to the network environment for our proposed algorithm so that it shows effective results against real proof DDoS traffics. Using the Reactive defence mechanism the data will be preventing for DDOS attack to the transmission of networks.

REFERENCE

[1] C. Schleher, Electronic Warfare in the Information Age. Artech House,1999.

[2] D. Wood and J. A. Stankovic, "Denial of service in sensor networks,"IEEE Comput., vol. 35, no. 10, pp. 54-62, 2002.

[3] J. Bellardo and S. Savage, "802.11 denial-of-service attacks: real vulnerabilities and practical solutions," in Proc. USENIX Security Symp., pp. 15-28, 2003.

[4] G. Noubir and G. Lin, "Low-power DoS attacks in data wireless LANs and countermeasures," SIGMOBILE Mob. Comput. Commun. Rev., vol. 7, no. 3, pp. 29-30, 2003.

[5] J. M. McCune, E. Shi, A. Perrig, andM. K. Reiter, "Detection of denialof-message attacks on sensor network broadcasts," in Proc. IEEE Symp.Security Privacy, 2005.

[6] W. Xu et al., "The feasibility of launching and detecting jamming attacks in wireless networks," in Proc. ACM Int'l. Symp. Mobile Ad Hoc Netw. Comput., 2005, pp. 46-57.

[7] W. Xu, T. Wood, W. Trappe, and Y. Zhang, "Channel surfing and spatial retreats: defenses against wireless denial of service," in Proc. ACM Workshop Wireless Security, pp. 80-89, 200

[8] Q.Huang, H.Kobayashi, and B.Liu. "Modeling of distributed denialof service attacks in wireless networks," in IEEE Pacific Rim Conf.Commun., Computers and Signal Process., vol. 1, pp. 113-127, 2003

[9] L.Sherriff, "Virus launches DDoS for mobile phones," [Online]. Available:

[10] Available: http:// www.scalable-networks.com/.

[11] Available: http://news.bbc.co.uk/

[12] available: http://games.slashdot.org/