Detecting Denail of Services Attacks in Wireless Network under the Distributed Jammer Network

P.Mohanraj, A.Mummoorthy
[1] Master of Computer Science and Engineering
K.S.R. College of Engineering, Tiruchengode, India
[2] Assistant Professor, Department of CSE
K.S.R. College of Engineering, Tiruchengode, India

ABSTRACT:
A Wireless network it's based on ad-hoc wireless networks, where each node transfers data to the neighbour nodes. AP (Access Point) need not be in the reach of all the nodes in the network. Nodes around the AP forward the packets from the distant nodes to the next node. They can work in a decentralized fashion, are cheap with minimum investment for initial infrastructure, more reliable, scalable and provide increased coverage. The denial of service attacks (DoS) have become more and more frequent and caused some fatal problems in the recent time. Internet users experience Denial of- service (DoS) attacks every day. We are going to present an Analytical approach which will employ Reactive Defence Mechanism to mitigate the DoS attack and further improve network performance in terms of less computation time. The distributed jammer network (DJN) is composed of a large number of tiny, low power jammers distributed inside a target network with the purpose of jamming the target network. Phase change or phase transition uses the percolation theory. In percolation theory nodes are setup using random process. Further the simulation result proves it to be a better result oriented approach.

Key Words
WN, Ad-hoc Network, DoS, Jammer, Access Point

1. INTRODUCTION
The wireless network can transfer the data threw the access point. The access point need not to be reach all the nodes in the network. Nodes around the AP forward the packets from the distant nodes to the next node. They can work in a decentralized fashion, are cheap with minimum investment for initial infrastructure, more reliable, scalable and provide increased coverage.

FIG: Wireless network components

1.1 Security in Wireless Network
A. confidentiality
Confidentiality is probably the most common aspect of information security. We need to protect our confidential information. Confidentiality not only applies to the storage of the information, it also applies to the transmission of information.

B. Integrity
Integrity means that changes need to be done only authorized entities. Integrity violation is not necessarily the result of a malicious act; an interruption in the system, such as power surge, may also create unwanted changes in some information.

C. Availability
The information created and stored by an organization needs to be available to authorized entities. Information is useless if it is not available. The unavailability of information is just as harmful for an organization as lack of confidentiality or integrity.

2. DENIAL OF SERVICES ATTACK
It is very common attack to wireless network. It may slow down or totally interrupt the denial of service attack. The attacker can use several strategies to achieve this. She might send so many bogus requests to a server that the server crashes because of the system heavy load. The attacker might intercept and delete a server's response to a client, making the client to believe that the server is not responding. The attacker may also intercept requests from the client, causing the clients to send requests many times and overload the system.

3. DISTRIBUTED JAMMER NETWORK (DJN)
Jammer is an electronic device used to disrupt the communication. DJN is composed of a large number of tiny, low power jammers distributed inside a target network with the purpose of jamming the target network. Jammer 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.

3.1 advantage of DJN
A. Robust
DJN is robust because it is composed of a large number of devices with ample redundancy

B .Low power
DJN notes emit low power which is advantageous because of health. DJN provides extended coverage with high energy efficiency.

3.2 Types of jammer
A .Constant Jammer
The constant jammer continually emits a radio signal. We have implemented a constant jammer using two types of devices. The first type of device we used is a waveform generator which continuously sends a radio signal. The second type of devices we used is a normal wireless device.

B. Deceptive Jammer
The deceptive jammer constantly injects regular packets to the channel without any gap between sup-sequent packet transmissions.

C. Random Jammer
Instead of continuously sending out a radio signal, a random jammer alternates between sleeping and jamming.

4. RELATED WORK

We set up a new kind of denial of service attack to wireless networks: distributed jammer network (DJN). 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.

5. CONCLUSION AND FUTURE WORK

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. In the case of DDoS attacks the attacker sends large volume of malicious packets which later prevent the legitimate user to access the services, therefore our prime concern is to find out the no of packets being malicious in the legitimate requests and then mitigates them by an appropriate mechanism. Using the Reactive defence mechanism the data will be preventing for DDOS attack to the transmission of networks.

6. REFERENCE

[1] PengT., Leckie, C. DoS, Ramamohanarao, K.: Survey of network-based defense mechanisms countering the and DDoS problems. ACM Computing Surveys **39**(1) (April 2007)

[2] Al-Duwairi, B., Manimaran, G.: Novel hybrid schemes employing packet marking and logging for IP traceback. IEEE Transactions on Parallel and Distributed Systems **17**(5) (May 2006) 403–418

[3] Dean, D., Franklin, M., Stubblefield, A.: An algebraic approach to IP traceback. ACM Transactions on Information and System Security **5**(2) (May 2002) 119–137

[4] Gong, C., Sarac, K.: Toward a practical packet marking approach for IP traceback. International Journal of Network Security (3) (May 2009) 271–281

[5] Li, J., Sung, M., Xu, J., Li, L.: Large-scale IP traceback in high-speed Internet: Practical techniques and theoretical foundation. 2006

[6] Snoeren, A.C., Partridge, C., Sanchez, L.A., Jones, C.E., Tchakountio, F., Kent, S.T., Strayer, W.T.: Hash-based IP traceback. In: Proceedings of the ACM SIGCOMM. (2001) 3–14

[7] Yu, S., Zhou, W., Doss, R., Jia, W.: Traceback of DDoS attacks using entropy variations. IEEE Transactions on Parallel and Distributed Systems **22**(3) (March 2011) 412–425

[8] Mitzenmacher, M., Upfal, E.: Probability and Computing: Randomized Algorithms and Probabilistic Analysis. Cambridge University Press (2005)

[9] CAIDA: Skitter project. http://www.caida.org/tools/measurement/skitter/