IJARES/Aug 2013/Volume-1/Issuse-1/Article No-5/26-31

INTERNATIONAL JOURNAL OF ADVANCED RESEARCH IN ENGINEERING AND SCIENCE

AN ASSESSMENT OF INTRUSION DISCOVERY SCHEMING FOR WIRELESS SYSTEM

T.Venu Gopal[1], P.Kavitha[2]

[1]**Dept of ECE, SV Engineering College, Hyderabad, A.P, India**

[2]**Dept of ECE, SV Engineering College, Hyderabad, A.P, India**

ABSTRACT:

The usage of wireless networks is growing in the modern days and is easy to build and priced reasonably. The most significant issues concerning each communication network is the security issues due to the confirmation of variety of attacks for the most part of which were targeting wired networks in view of the fact that wireless networks weren't that much extensive all the way through earlier time. Wireless networks are compromised more easily when compared to any other wire line networks and is the main drawback of it. For an adversary to set up an attack of denial of service was made simple by means of the service of the transition in wireless networks. In order to discover the existence of an adversary node, numerous schemes were projected for the purpose of defending from the attacks. In order to block the accessing by means of wireless nodes to the medium, a radio signal is broadcasted repeatedly by the jammer. The techniques of jamming will show the difference from the simple to more complicated are based on the constant transmission of the signals of the interference which depend on the employing of the protocol used for the contact between the wireless devices.

KEYWORDS: Jamming Attacks, Wireless Networks, Adversary Node, Denial of Service Attack.

1. INTRODUCTION:

Due to the recent advancements made in the wireless technology has increased the usage of wireless networks and are priced reasonably and can be built easily. The most significant issues concerning each communication network is the security issues due to the confirmation of variety of attacks for the most part of which were targeting wired networks in view of the fact that wireless networks weren't that much extensive all the way through earlier time [2] [8]. Some simple modifications were made at the media access control protocol and in order to avoid jamming; we can integrate to the system approaches. Wireless networks are compromised more easily when compared to any other wire line networks and is the main drawback of it [11]. To block the sense of communication connecting the two capable wireless nodes, it is realistic. To attain the task devoid of being identified, jammers can possibly exist in numerous intellectual ways. To preferentially obtain the interference aimed at corrupting the particular packet, the transmission of a control packet and the jammer was discovered. For an adversary to set up an attack of denial of service was made simple by means of the service of the transition in wireless networks [1]. In order to discover the existence of an adversary node, numerous schemes were projected for the purpose of defending from the attacks [5]. Numerous models of jamming were made available and they have been established to be very effectual regardless of their openness. Regarding the insertion of the changeability at the dimension and timing of the important packet controls, the privacy of our complex can possibly be improved by means of execution of the mentioned methods [9]. The techniques of jamming will show the difference from the simple to more complicated are based on the constant transmission of the signals of the interference which depend on the employing of the protocol used for the contact between the wireless devices [14]. There is no solution which can presently address to the trouble of jamming in wireless networks and is the most important conclusion. Initially the subsystem can operate at the physical layer and can make the usage of checks of consistency and later on the second subsystem will identify the probable malicious action of the intelligent jammers at the media access control layer and in this way the action of detection can be completed in two levels [3] [6].

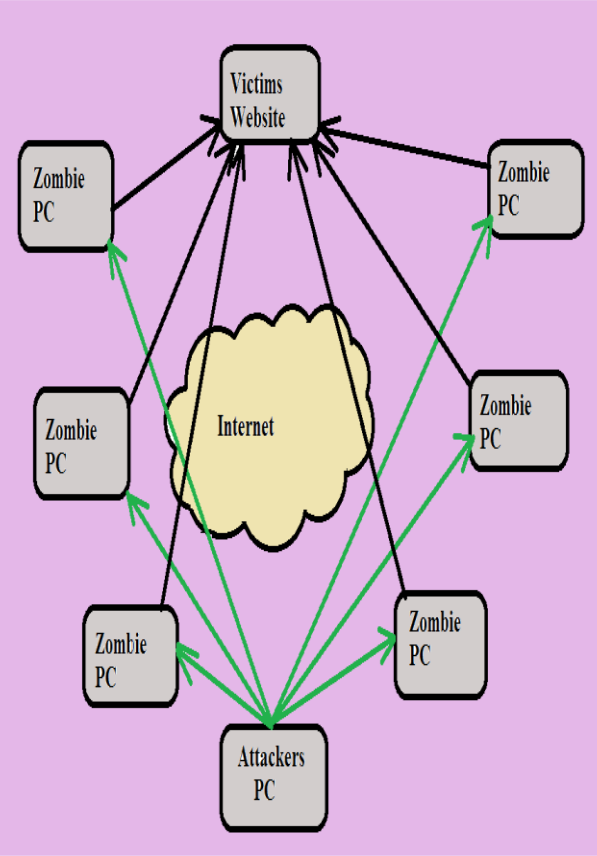

Fig 1: Denial of Service Attacks

The situation of jamming will describe about the appropriate standards in order to measure the different methods of jamming for a particular circumstances. For sensor nodes, the energy excellence may possibly be the most important metric and for the extensive time the nodes are accepted to survive [4].

2. DETECTION OF ATTACKS IN WIRELESS NETWORKS:

Even though numerous attacks were shown in fig1 for wireless networks occur at the layer of the media access control and hence it is difficult to use them in the schemes of the intrusion detection and to separate the packet sequences. In order to avoid the user in a translucent way, most of the systems that are proposed understand about the intruder [10]. In anticipation of current days, most of the work that has been done refers to the intrusion prevention. For wired networks, the schemes of intrusion detection have been tremendously examined and most of them are put into practice for a wired network is signature based. For the mobile user, the limitation of the power of a mobile user is such that to manufacture such a system making it more complicated that requires for the storage of a great quantity of signature attacks [7] [13]. Wireless Intrusion Detection Systems is the detection scheme proposed for the wireless networks. Domino can be organized to make known about the methods of the comparable which are used by the adversaries and it compact by means of the legitimate users of the avaricious. This system does not require any modification on the active infrastructure is the vast advantage and notices numerous

types of attacks and also runs at the access point only.

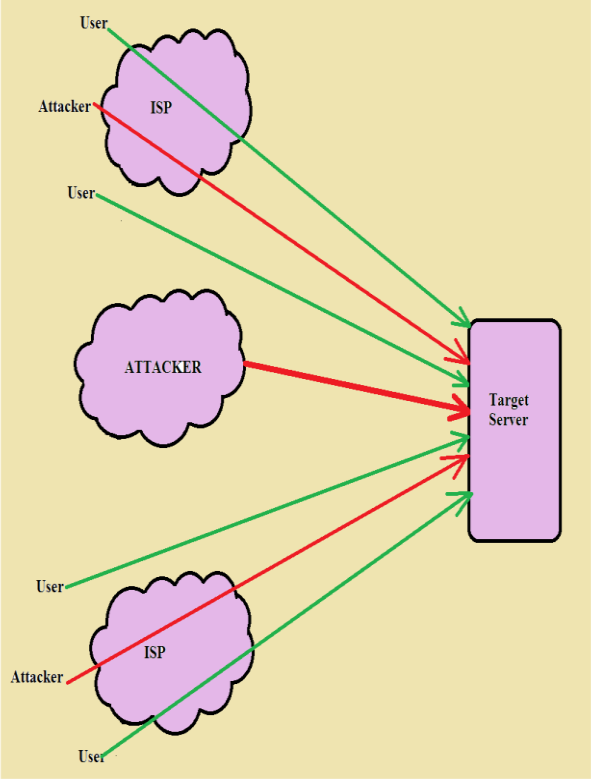

Fig 2: An overview of Denial of Service Attacks

In the fundamental concept of a scheme of the wireless distributed intrusion detection if the embarrassment of the performance is mainly because of breakdown of the network or due to a jamming, a node cannot make a decision attack on itself [12]. The ongoing traffic was monitored by the each node in the network and list of verification is generated which occurs on the network of the wireless medium. In order to achieve a denial of service attack shown in fig2 an opponent can makes usage of the media access control. All the nodes need to assist to take a precise decision. The user who tries to receive the admission to the channel more frequently can be noticed by the system and it outcomes the more bandwidth or put off from the usage of the medium from the others as a result causing attacks of denial service.

3. INTRUSION ANTICIPATION METHODS:

The usage of systems of intrusion hindrance is moreover prevalent in wireless networks and is the initial line of security for a wireless network and these systems attempt to avoid anti jamming and presume that there is antagonist at the network. The various schemes of anti jamming are as follows: protecting of network from a Layer jamming attack is a method which is straight forward and builds the network and is more protected against such attacks. Aggregate multiple packets is a method foils the dependability of the packet sequence. A paddling method is used effortlessly by making the size of the each packet control of similar size for the packets and as a consequence harder to be recognizable. An anti jamming technique which tries to get

the advantage of the mobility of the nodes is known to be spatial retreats. The node initiates the touching out of the blocked area and executes the algorithm of detection at the same time when it senses that it is being jammed. On the other hand the node runs off initially from the area of jamming and it attempts to stay on connected with the relax networks when it is being blocked in order to keep away from the partition of the phase of the rebuilding of the network. The method which is stimulated from the technique of the incidence hopping in some way is known as channel surfing and occurs at the media access control layer different from the frequency hopping that occurs at the physical layer. The nodes exchange the channel and send a beacon communication at the occurrence of the new band when it is blocked. The neighbours of the non-jamming will amend the channel in an attempt and observe if their neighbours had broadcast beacon at the channel and experience the absence of the node.

4. CONCLUSION:

The most significant issues concerning each communication network is the security issues due to the confirmation of variety of attacks for the most part of which were targeting wired networks in view of the fact that wireless networks weren't that much extensive all the way through earlier time. There is no solution which can presently address to the trouble of jamming in wireless networks and is the most important conclusion. Initially the subsystem can operate at the physical layer and can make the usage of checks of consistency and later on the second subsystem will identify the probable malicious action of the intelligent jammers at the media access control layer and in this way the action of detection can be completed in two levels. Regarding the insertion of the changeability at the dimension and timing of the important packet controls, the privacy of our complex can possibly be improved by means of execution of the mentioned methods. Some simple modifications were made at the media access control protocol and in order to avoid jamming; we can integrate to the system approaches.

REFERENCES:

[1] L.Sherriff, Virus launches DDoS for mobile phones,
http://www.theregister.co.uk/content/l/12394.html

[2] Wenyuan Xu, Wade Trappe, Yanyong Zhang, Timothy Wood, The Feasibility of Launching and Detecting Jamming Attacks inWireless Networks,

MobiHoc 05, May 25-27, 2005, Urbana-Champaign, Illinois, USA, pp 46- 57.

[3] Y. Law et al., Link-Layer Jamming Attacks on S-Mac, Proc. 2nd Euro. Wksp. Wireless Sensor Networks, 2005, pp. 21725.

[4] Wenyan Xu, Ke Ma, Wade Trappe, Yanyong Zhang, Jamming Sensor Networks: Attacks and Defense Strategies, IEEE Network, May/June 2006.

[5] A.Mishra, K.Nadkarni, A.Patcha, Intrusion Detection inWireless Ad Hoc Networks, IEEE Wireless Communications, February 2004.

[6] P.Kyasanur, N.Vaidya, Selfish MAC Layer Misbehavior in Wireless Networks, IEEE transactions on mobile computing, Vol.4, No5, September/ October 2005.

[7] G.Noubir, G.Lin, Low Power DoS Attacks in Data Wireless LANs and Countermeasures, in Proceedings of Poster: ACM MobiHoc 2003. Annapolis, MD: ACM Press.

[8] A. Wood and J. Stankovic, Denial of Service in Sensor Networks, IEEE Comp., vol. 35, no. 10, Oct. 2002, pp. 5462.

[9] G.Noubir, On Connectivity in Ad Hoc Networks under Jamming Using Directional Antennas and Mobility, Technical Report, December 2003.

[10] Curtis D. Schleher, ElectronicWarfare in the Information Age, 1999, Norwood, Artech House.

[11] T.X.Brown, J.E.James, A.Sethi, Jamming and Sensing of Encrypted Wireless Ad Hoc Networks, MobiHoc06, 22-25 May, Florence-Italy.

[12] Schiller, Mobile Communications, Addison-Wesley Longman Publishing, Boston, 1999.

[13] J.Bellardo, S.Savage, 802.11 Denial-of-Service Attacks: Real Vulnerabilities and Practical Solutions, In Proceedings of USENIX Security Symposium03, August 03.

[14] M.Raya, I.Aad, J-P.Hubaux, A. El Fawal, DOMINO: Detecting MAC layer greedy behavior in IEEE 802.11 hotspots, in Proceedings of ACM MobiSys, Boston (MA), USA, 2004