Novel Method to Overcome Vulnerability in Wi-Fi Network

Basil Peter[1], Nisanth Krishnan[2]

[1]Faculty, Dept. Of Physics, Triumphant Institute of Management Education Pvt. Ltd., Kerala, India
[2]Assistant Professor, Dept. ECE, Toc H Institute of Science and Technology, Kerala, India

---***---

Abstract - *Wireless networks are prone to security attacks. Security issues have increased proportionally as the number of users increased. One of the major security issues witnessed is Denial-of-Service (DoS) attack. Denial-of-Service (DoS) attack is an attempt to make a machine or network resource unavailable to its intended users, such as to temporarily or indefinitely interrupt or suspend services of a host connected to the Internet. To prevent DoS attacks, in the proposed scheme instead of the randomly chosen initial sequence number which can generally be predicted, we enter the sequence number of our own choice as the initial sequence number. The effect of Denial of Service attack on a normal network is then analyzed and the performance of the proposed scheme is evaluated by measuring the throughput, number of packets received and number of packets lost by implementing it in NS2.*

Key Words: Denial of Service Attack, Mac Spoofing, Access Point, WLAN, TCP, UDP.

1. INTRODUCTION

The popularity of wireless Networks is a testament primarily to their convenience, cost efficiency, and ease of integration with other networks and network components. The benefits of wireless networks include: Convenience, Mobility, Productivity, Deployment, Expandability and Cost. Wireless Network technology, while replete with the conveniences and advantages described above has its share of downfalls. The disadvantages of using a wireless network are: Security, Range, Reliability, and Speed. Wireless Networks present a host of issues for network managers. Unauthorized access points, broadcasted SSIDs, unknown stations, and spoofed MAC addresses are just a few of the problems. One of the major and increasingly used attacks for network disruption is Denial of Service attack.

1.1 Denial of Service Attack (DoS)

Denial of Service Attack, according to Chung-Hsin Liu et al (2010) is an attempt by the hacker to utilize the network in place of the authenticated user [1]. A Denial-of-Service attack (DoS) occurs when an attacker continually bombards a targeted AP (Access Point) or network with bogus requests, premature successful connection messages, failure messages, and/or other commands. These cause legitimate users to not be able to get on the network and may even cause the network to crash. These attacks rely on the abuse of protocols such as the Extensible Authentication Protocol (EAP). The United States Computer Emergency Readiness Team (US-CERT) defines symptoms of denial-of-service attacks to include, unusually slow network performance (opening files or accessing web sites), unavailability of a particular web site, inability to access any web site etc.

Zhang Laishun et al (2010) suggested a client puzzle based defense mechanism to resist Dos attacks in WLAN. In this method before engaging in any resource consuming operations, the server first generates a puzzle and sends its description to the client that is requesting service from the server. The client has to solve the puzzle and send the result back to the server. The server continues with processing the request of the client, only if the client's response to the puzzle is correct. The methodology proved to be an efficient and lightweight mechanism to defend against DoS attacks on 802.11 networks. The method can defend against authentication and association attacks however the fact that the scheme was tested only under experimental network, its efficiency in the real network scenario is questionable [2].

Kavitha C et al (2014) proposed a a secured alternative path routing protocol against DoS attack which prevents and detects the DoS attack in sensor network [3]. Keiichirou Kurihara et al (2014) proposed a detection method with only 2 header information that is fewer than conventional methods: —packet arrival time and —source IP address [4]. M.Padmadas et al (2013) proposed a RTB Rule Based Adaptive Selective Verification Protocol To Prevent DoS Attack [5]. The proposed system RTB Rule on Server Side Based on ASV used a protocol which is highly adaptive to the arriving attack rates. However it's found that these schemes are not very efficient in preventing Denial of Service Attacks.

The scheme proposed in this paper can be used to modify the sequence number field. Instead of the randomly chosen initial sequence number which can generally be predicted, in the proposed scheme we can enter the sequence number of our own choice as the initial sequence number. This can prevent Denial of Service Attacks to a great extent.

1.2 AODV Routing Protocol

The Ad hoc On-Demand Distance Vector (AODV) algorithm enables dynamic, self-starting, multihop routing between participating mobile nodes wishing to establish and maintain an ad hoc network. AODV allows mobile nodes to obtain routes quickly for new destinations, and does not require nodes to maintain routes to destinations that are not in active communication. AODV allows mobile nodes to respond to link breakages and changes in network topology in a timely manner.

The operation of AODV is loop-free, and by avoiding the Bellman-Ford "counting to infinity" problem offers quick convergence when the ad hoc network topology changes (typically, when a node moves in the network). When links break, AODV causes the affected set of nodes to be notified so that they are able to invalidate the routes using the lost link. One distinguishing feature of AODV is its use of a destination sequence number for each route entry. The destination sequence number is created by the destination to be included along with any route information it sends to requesting nodes. Using destination sequence numbers ensures loop freedom and is simple to program. Given the choice between two routes to a destination, a requesting node is required to select the one with the greatest sequence number.

2. METHODOLOGY

The Denial of Service attack is an attempt to make computer resources unavailable to its legitimate users. In the proposed scheme, when the source node is sending a packet to the destination node, it will be checked in the ICT (Intruder Check Table) to see whether the system trying to communicate is a member of the WLAN group. If the Mac address is present in Intruder Check Table then the user will be allowed to communicate within the wireless local area network. If the packet is suspicious but unerring, the requested packet will be redirected to BNS (Basil Numbering Scheme) via ICT to avoid the false positive. When the BNS scheme is initialized the user will be asked to enter the initial sequence number. The following sequence numbers will be based on the initial sequence number we have entered. Once we enter the initial sequence number, the next sequence number is chosen automatically by incrementing a value of 2, with the previous value of sequence number. This is an improvement over the scheme in which the sequence number is randomly chosen. In BNS mechanism, the hackers cannot easily assume the exact initial sequence number and the alternative numbers present in the header field unlike in a normal sequence number based scheme to make MAC spoof attack.

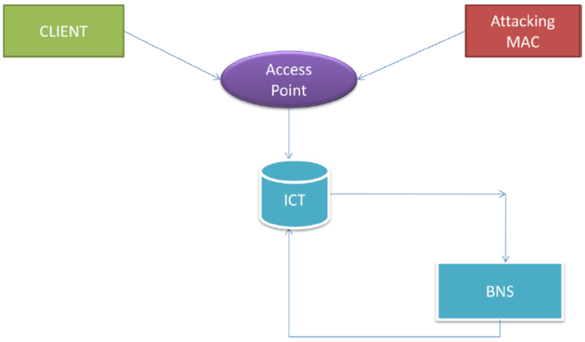

Fig -1: Method to prevent Denial of Service Attack

3. EXPERIMENTS AND RESULTS

All the simulations have been performed on Ubuntu as the Operating System. NS 2.35 has been installed on the platform for simulation.

Table -1: Simulation Set Up

Simulation Setup Routing protocol	AODV
Topography	3800*5379 m^2
Transmitted Power	10.031622777 dB
Antenna Model	Omni antenna
No. of mobile nodes	62
No. of user nodes	3
No. of attackers	58
Traffic type	CBR
Simulation time	110s
MAC protocol	IEEE 802_11

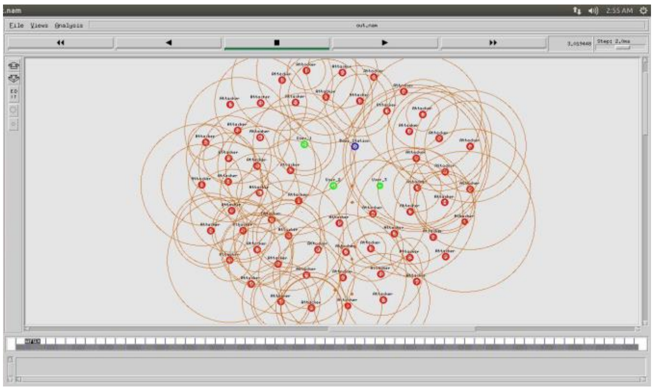

Fig -2: Nam Window showing user under attack

The Nam window in figure 2 shows the network topology with one base station node and three user nodes, where the second user is attack by 58 attacking agents. The attacking agents continuously bombard the user node 2 with a lot of unwanted information which leads to drop in the network performance, as the user node is kept busy with unwanted traffic.

To understand the extent of improvement of network performance with the application of Basil's Numbering Scheme, a comparison is done between a network under Denial of Service attack and a system making use of BNS when under Denial of Service attack.

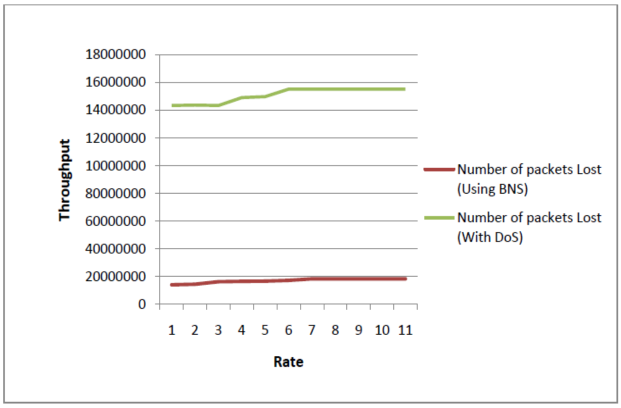

Chart -1: Plot of Throughput Vs Rate

It is seen that the throughput becomes almost zero as a result of the denial of service attacked carried out by 58 attacking nodes. Whereas when the BNS scheme is initiated the network performance improves significantly. In fact, using BNS enables us to achieve a efficiency of close to 100%.

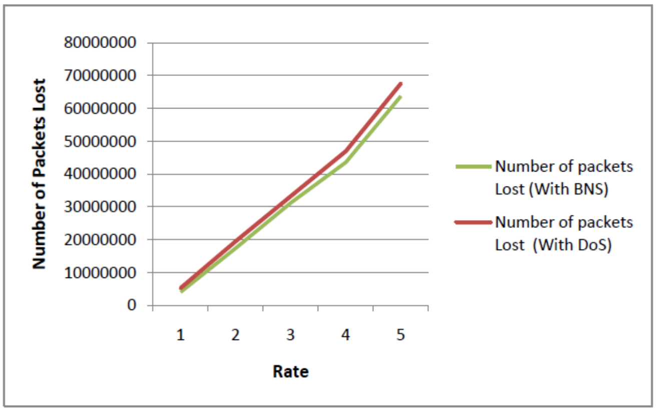

Chart -2: Plot of Packet Loss Vs Rate

It is observed that the number of packets lost steadily increases when the network is under denial of service attack. However upon the application of Basil's Numbering Scheme, it observed that the number of packets lost decreases as a result of the scheme. This means that the communication process takes place effectively without much loss of packets of data.

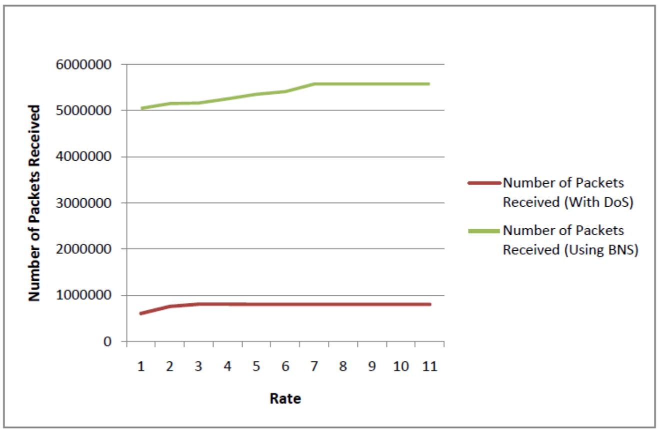

Chart -3: Plot of Packet Received Vs Rate

As seen from the above graph the number of packets received when a node is under denial of service attack is significantly decreased. Now on the application of Basil's Numbering Scheme the number of packets received has shown a significant improvement. Almost all the transmitted packets are being received, which means that there is no loss of data taking place.

4. CONCLUSIONS

The Denial of Service Attack will block out the legitimate users from the network and it causes a denial of availability of the network resources to the user. From the results it is seen that the proposed BNS scheme can effectively thwart Denial of Service attack to a great extent. This is achieved by choosing the initial sequence number of our own choice thereby limiting the possibility of a third party getting hold of our initial sequence number. Human thoughts and behavior being random will enable the user to choose a random initial sequence number and hence overcoming the possibility of an exact guess of the ISN.

Once the initial sequence number is chosen, the sequence number is incremented by a value of 2 for every subsequent packet of transmission. This makes it difficult for the attacker to guess correctly the series of sequence numbers o carry out the attack. With an additional mechanism to block the earlier hackers out of the network immediately as their Mac address of the registered users will be intruder check table, this scheme can defend against sequence number based denial of service attacks. The analysis was done to understand the effectiveness of BNS in preventing it. It was evaluated in network simulator 2 and the performance was compared against parameters like throughput, number of packets lost and packets received

REFERENCES

[1] D. Chung-Hsin Liu & Yong-Zhi Huang, ―The analysis for DoS and DDoS attacks of WLAN‖ , In Proc of IEEE Second International Conference on MultiMedia and Information Technology, pp.108-111, 2010

[2] Zhang Laishun, Zhang Minglei, & GuoYuanbo, ― A Client puzzle based defense mechanism to resist DoS attacks in WLAN‖, In Proc of IEEE International Forum on Information Technology and Applications., pp. 424-427, 2010

[3] M. Shashikala & Dr. Kavitha. C, ―A Secured Alternative path Routing Protocol against DoS attack‖, In Proc of IEEE Eleventh International Conference on Wireless and Optical Communications Networks (WOCN), pp.1-5, 2014.

[4] Keiichirou Kurihara & Kazuki Katagishi, ―A Simple Detection Method for DoS Attacks based on IP Packets Entropy values‖, In Proc of IEEE Ninth Asia Joint Conference on Information Security, pp.44-51, 2014.

[5] M.Padmadas ,Dr.N.Krishnan & Sreeja Nair M.P, ― RTB Rule Based Adaptive Selective Verification Protocol To Prevent DoS Attack‖, In Proc of IEEE International Conference on Computational Intelligence and Computing Research ,pp.1-5, 2013.

BIOGRAPHIES

Faculty in Physics at Triumphant Institute of Management Education Pvt. Ltd. Has done M.Tech In Electronics with Specialization in Wireless Technology under CUSAT.