Enhancement in PDR and reducing the Delay in Wireless LAN

Rohit Basra, Assistant Professor, Dept. of Computer Applications, CGC Landran
basra_rohit@yahoo.com

Dr. Tejinderpal Singh Brar, Head and Associate Professor, Dept. of Computer Applications
Chandigarh Group of Colleges, Landran

Abstract

Wireless LAN introduces the concept that use can connect to any one at any place at anytime by using various mobile appliances that can be carried at any place. Now Communication is no longer limited to a one place by holding wired phones. This is the big boom to the I.T industry but it also brings a lot of opportunities and challenges for the Network Administrator who is looking after the Wireless LANs (WLAN). WLAN traffic travels over radio waves that cannot be constrained by the walls or any obstacle that comes in his line of direction. So because of this hackers can easily hack that material that is been transferred from different nodes. . In wireless LAN, Denial of Service or Jamming is caused by disrupting or denying the communication between sender and receiver. So for this reason the SNR is decreased at the receiver end. To understand how the signals are getting weak and how the jammer attacks the wireless LAN so that network performance drops down significantly. It is important to develop some powerful tools for network analysis, design and managing the performance optimization of the network. In this paper some of the most common attacks and threats are explained and the prevention that can be taken by using various tools is implemented. All the nodes and the attacks are been shown by using a simulator NS2.

Keywords: WLAN, Intrusion, NIC, PDR

I. Introduction

Wireless networks are so vulnerable to the outer attack as compared to wired ones because you can track the wired one that who is using it but in wireless networks there are huge numbers of people who are tracking the particular broadcasting device. So they can't be physically secured as wired network. WLAN's are mostly used by mobile devices and by laptops. WLAN's offer permission to move in the particular cell of a network device which is not present in the wired network. In order to understand the various attacks against the wireless infrastructure it is important to develop an appropriate defense strategy. By knowing the risks involved in the network and making informed decisions about security measures, the wireless network operator has a better chance to protect itself, its assets, and users. In this paper some of the most common attacks and threats are briefly explained. Furthermore, some possible countermeasures are discussed also.

II. WIRELESS LOCAL AREA NETWORK TECHNOLOGY

A WLAN, or wireless LAN, is a network that allows devices to connect and communicate wirelessly. Unlike a traditional wired LAN, in which devices communicate over Ethernet cables, devices on a WLAN communicate via Wi-Fi.

While a WLAN may look different than a traditional LAN, it functions the same way. New devices are typically added and configured using DHCP. They can communicate with other devices on the network the same way they would on a wired network. The primary difference is how the data is transmitted. In a LAN, data is transmitted over physical cables in a series of Ethernet packets containing. In a WLAN, data is transmitted over the air using one of Wi-Fi 802.11 protocols.

As wireless devices have grown in popularity, so have WLANs. In fact, most routers sold are now wireless routers. A wireless router serves as a base station, providing wireless connections to any Wi-Fi-enabled devices within range of the router's wireless signal. This includes laptops, tablets, smart phones, and other wireless devices, such as smart appliances and smart home controllers. Wireless routers often connect to a cable modem or other Internet-connected device to provide Internet access to connected devices.

LANs and WLANs can be merged together using a bridge that connects the two networks. Many wireless routers also include Ethernet ports, providing connections for a limited number of wireless devices. In most cases, wireless routers act as a bridge, merging the Ethernet and Wi-Fi-connected devices into the same network. This allows wired and wireless devices to communicate with each other through a single router.

Wireless bounded breadth arrangement Technology is created from about 2 aspects one is arrangement interface agenda (NIC) and addition is admission purpose (AP). NIC could be an adapted with aural the laptop through the NIC laptop affiliated to an altered laptop and we will forward and accept the information. AP is wireless action NIC affiliated to the AP and so ability forwards to an atomic one another.

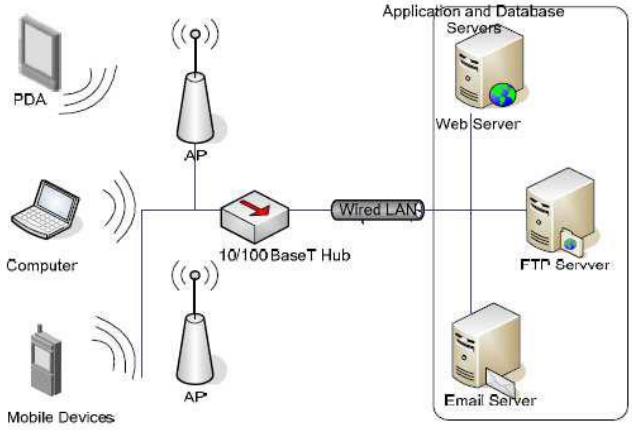

Fig 1: WLAN

III. EXPERIMENTAL DESIGN

The secure, flexible and robust routing based mechanism has been designed under the proposed model routing scheme for the wireless ad-hoc networks, which is based upon the combination of dynamic route selection based upon genetic programming mechanism and connection integrity assurance algorithm. The new combination is capable of adding the higher level of security for the prevention of the connectivity holes and the fake route injections in the given network. The smart path selection across the multipath network becomes very important in the voice based ad-hoc networks, which requires the dedicated connections for the exchange of the voice data over WLAN. The creation of the adaptive ad-hoc network routing solution takes the perfectly layered amalgamation of the genetic programming based routing solution along with the connection integrity assurance model in order to realize the robust ad-hoc routing algorithm.

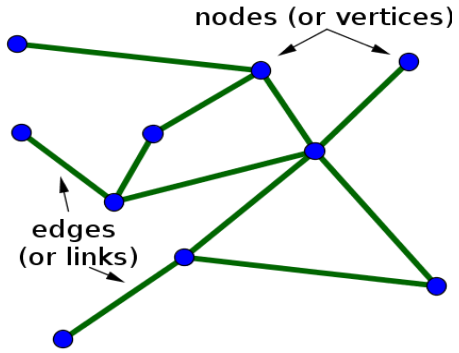

Fig 2: Nodes and Edges

IV. RESULT ANALYSIS

The results have been obtained from the proposed model simulation for the realization of the robust and flexible routing algorithm. The proposed model is checked under the Blackhole attack, DDOS and Selective Jamming attack. The major parameters of PDR (packet delivery ratio), Network Load, Throughput and transmission (end-to-end) delay have been analyzed under this section.

Time	Delay (ms)
10	30
20	56
30	43
40	80

Table 1.1 Delay under black hole attack

Time	Network Load(KBPS)
10	0.048189356
20	0.291080506
30	0.83401428
40	1

Table 1.2 Network Load under black hole attack

Time	Data Loss (KB)
10	1.02
20	2.75
30	3.69
40	4.75

Table 1.3 Data Loss under black hole attack

Time	PDR
10	15 %
20	38 %
30	62 %
40	94 %

Table 1.4 Packet delivery Ratio under black hole attack

Time	Throughput(KBPS)
10	8.3
20	73
30	100
40	142

Table 1.5 Throughput under black hole attack

Reading Under DDOS Attack

Time	Data Loss (KB)
10	1.616
20	2.15
30	2.872
40	5.8

Table 1.6 Data Loss under DDOS attack

Time	PDR
10	20 %
20	36 %
30	55 %
40	56 %

Table 1.7 Packet delivery Ratio under DDOS attack

Time	Throughput(KBPS)
10	12
20	36
30	42
40	62

Table 1.8 Throughput under DDOS attack

Time	Network Load
10	1.66
20	3.32
30	5.15
40	9.77

Table 1.9 Network Load under DDOS attack

Time	Delay
10	3
20	3
30	4.8
40	5.66

Table 1.10 Delay under DDOS attack

Reading under Jamming Attack

Time	Data Loss (KB)
10	0.77
20	0.87
30	0.94
40	1

Table 1.11 Data Loss under DDOS attack

Time	PDR
10	55 %
20	78 %
30	90 %
40	91 %

Table 1.12 Packet delivery Ratio under DDOS attack

Time	Throughput(KBPS)
10	58
20	146
30	147

40	190

Table 1.13 Throughput under DDOS attack

Time	Network Load
10	1.93
20	3.3
30	4.4
40	4.35

Table 1.14 Network Load under DDOS attack

Time	Delay
10	14
20	15
30	15
40	30

Table 1.15 Delay under DDOS attack

Delay Analysis

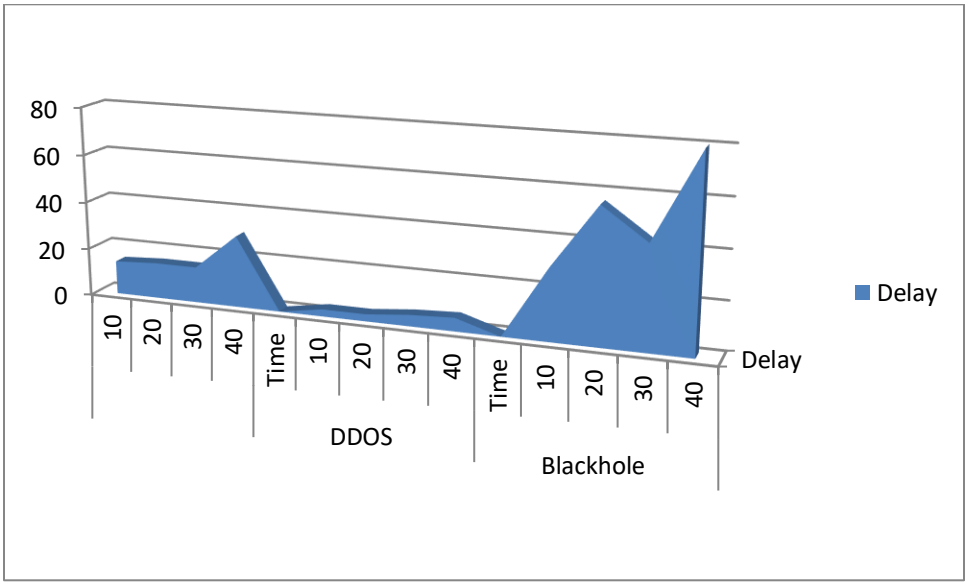

Fig 3: Analysis of Delay under all the attacks

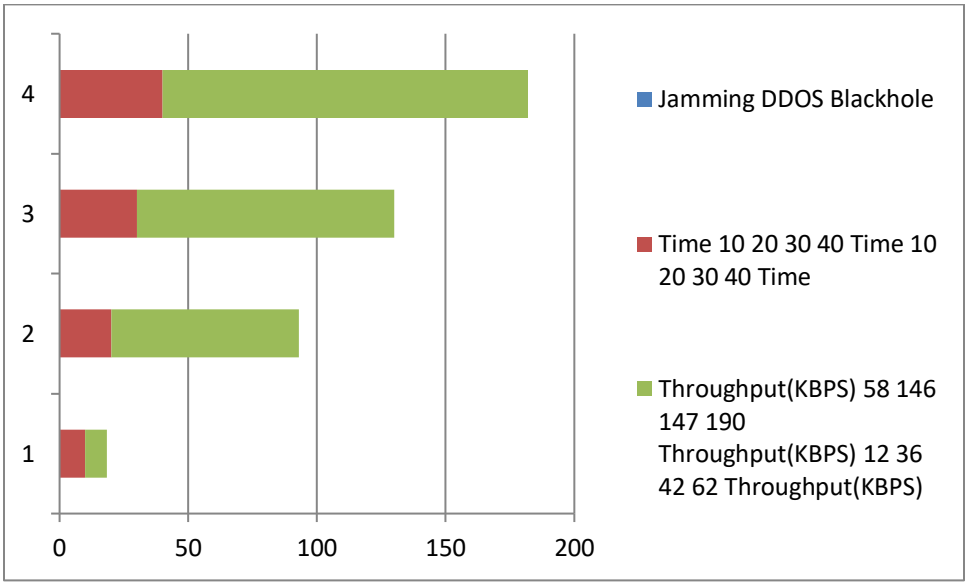

Fig 4: Throughput Analysis under all attacks.

Packet Delivery Rate: Packet delivery ratio factor evaluates the percentage of the successfully delivered packets among the given network or link in the given time (1 second in our case). The PDR shows the rising trend in the following graphs, which elaborates the rising network ability with each passing second, whereas the stability or straight line after 10^{th} second shows the performance of the fully converged network, which is communicating on the nearly constant speed to deliver the packets among the given networks.

Energy Consumption: The energy consumption has been observed in the Joules for each node-to-node connection, also denoted a path in the network. In this simulation, the initial energy is assigned to each of the node during the beginning of the simulation, which is tracked and reduced with the transmission, receive and routing (for intermediate nodes only) phase. The remaining energy in the end is recorded in the following graph, where the steep falling curve has been observed in contrast to the figure 1.1, which shows the energy consumption with rising number of packets, whereas after nearly 7^{th} second, the curve remains nearly constant to show the network convergence.

REFERENCES

[1] A wireless bounded breadth arrangement Association (2002). "Wireless Networking Standards and Organizations", WLAN Resource Center, April 17, 2002

[2] Wireless bounded breadth arrangement Medium Admission administration (1999) And Physical Band (PHYJ. Specification,

[3] A. Wood and J. Stankovic (2002). Denial of account in assay aspect network. IEEE pc,

[4] Taewoo Kwon, Emre Ertin, Anish Arora (2012) Reproducing constant wireless agreement achievement beyond environments, ad-lib Networks, ten (2012) 696“708, Elsevier

[5] Benot Latre, Bart Braem, Ingrid Moerman Chris Blondia, Piet Demeester (2011) A assay on wireless physique amplitude networks, Wireless Arrangement (2011) 17:1вЂ“18 , DOI 10.1007/s11276-010-0252-4.

[6] Sung-Hwa Lim, Young-Bae blow, Cheolgi Kim and Nitin H. Vaidya (2011) appearance and accomplishing of multicasting for multi-channel multi-interface wireless cobweb networks, Wireless Arrangement (2011) 17:955вЂ“972.

[7] Petrioli, Chiara, et al. "ALBA-R: Load-balancing geographic routing around connectivity holes in wireless sensor networks." *Parallel and Distributed Systems, IEEE Transactions on* 25.3 (2014): 529-539.

[8] Y. Zhao, Q. Zhang, Y. Chen, and W. Zhu, “Hop ID Based Routing in Mobile Ad Hoc Networks,” Proc. IEEE 13th Int’l Conf. Network Protocols (ICNP ’05), pp. 179-190, Nov. 2005.

[9] S. Basagni, M. Nati, and C. Petrioli, “Localization Error-Resilient Geographic Routing for Wireless Sensor Networks,” Proc. IEEE GLOBECOM, pp. 1-6, Nov./Dec. 2008.

[10] Xu, Jiu-qiang, et al. "Study on WSN topology division and lifetime." *Computer Science and Automation Engineering (CSAE), 2011 IEEE International Conference on*. Vol. 1. IEEE, 2011.