

## “Experimental Measurements of Bandwidth under IEEE 802.11b Wireless Local Area Networks”

(1) Dr. Atul M Gonsai (Asst. Professor)\*

\*Dept of Computer Science, Saurashtra University, Rajkot360005, Gujarat, India.

### Abstract:

The market for wireless communications has experienced incredible growth over recent years. Wireless Local Area Networks (Wireless LANs) have quickly found a significant place and popularity in business and the computer industry. The major benefit of wireless LANs is increased flexibility and mobility. This research investigated the effect of multiple security mechanisms on the performance of congested and un-congested networks. The effect of different TCP and UDP packet sizes on performance of secure networks was also studied. The results showed that WEP encryption significantly degrades the performance of wireless networks.

### 1 Wireless Networks

Wireless technologies have quickly found a significant place and popularity in business and the computer industry. Their major motivation and benefit is increased flexibility and mobility. Unlike a traditional wired network, which requires a wire to connect a computer to the network, wireless technology enables the users to access information from anywhere without any restriction. Wireless networks are frequently categorized into three groups based on their coverage range [1]: Wireless Wide Area Network (WWAN), Wireless Local Area Network (WLAN), and Wireless Personal Area Network (WPAN).

Wireless LANs provide greater flexibility and portability than do traditional wired LANs. Unlike a wired LAN, which requires a wire to access the network, a Wireless LAN connects computers and other components to the network via an Access Point (AP). IEEE 802.11 is an international standard providing transmission speeds ranging from 1 Mbps to 54 Mbps in either the 2.4 GHz or 5 GHz frequency bands.

### 2 Bandwidth of 802.11 Wireless LANs

The 802.11b standard is generally understood as an 11 Mbps Ethernet LAN running in the 2.4 GHz ISM radio band. Because of the demands of the protocol, and the multiple factors influencing radio signals, it is very unlikely that the users will ever achieve 11 Mbps as an operational bandwidth on their LANs. The theoretical throughput can be attained is 75% of the nominal bit rate [2], although a target of 65% is commonly observed. Applying this formula to an 11 Mbps 802.11b network, this yields a practical throughput in the range of 6 to 8 Mbps. A comparison test was carried out on the 802.11a and 802.11b throughput limits [3]; the author observed the limit for 802.11a was 30.34 Mbps and 6.44 Mbps for 802.11b. The maximum overall throughput of an 802.11b Wireless LAN in a similar study [4] was reported to be about 6.45 Mbps with a standard deviation of 0.02 Mbps for a single station. Another study [5] analyzed IEEE 802.11 operation under various assumptions such as time-independent modeling, geometrically distributed packet sizes, etc. Those results also showed that the IEEE 802.11 standard operates at rates lower than a theoretically possible 7.27 Mbps. The actual amount of bandwidth is largely dependent on interference and frequency congestion.

### 3 Wired Equivalent Privacy (WEP)

Interception of radio communications has been a problem for as long as radios have been used to transmit sensitive information. Since radio transmissions travel in unsecured areas, interception of these radio signals by an attacker is a real threat. In order to protect the data from eavesdroppers, various forms of encryption have been used.

The 802.11 MAC specifications describe an encryption protocol called Wired Equivalent Privacy (WEP). The goal of WEP is to make Wireless LAN communication as secure as wired LAN data transmissions. WEP provides two critical pieces to the wireless security architecture: authentication and confidentiality. It uses a shared key mechanism with a symmetric cipher called RC4 11. The key that a client is using for authentication

and encryption of the data stream must be the same key that the AP uses. The 802.11 standard specifies a 40-bit key, however most vendors have also implemented a 104-bit key for greater security.

Encryption of the data stream provides confidentiality of the data transmitted between two Wireless LAN devices. The encryption mechanism used in WEP is a symmetric cipher; this means that the key, which is used to encrypt the data, is the same key that will decrypt the data. If both wireless LAN devices do not have the same encryption key, the data transfer fails.

#### 4 Wireless Performance

Security is a property of an entire system and every decision must be examined with security in mind [6]. There have been many evaluation studies of IEEE 802.11 wireless network performance; however, little attention has been paid to the effects of implementing security on performance. Some relevant evaluation studies have been described in this section.

Amaro et al. [7] evaluated the performance of wireless networks and concluded that, the larger the packet size, the higher the effective rate. The collision avoidance mechanism of 802.11b protocol confirmed this increase, as traffic overheads introduced by the control frames and the ACK frames diminished for larger packets.

An empirical characterization of the instantaneous throughput of a station in an 802.11b Wireless LAN, as a function of the number of competing stations sharing the AP, was presented in [8]. The results showed that as the number of stations increases, the overall throughput decreases and its variance increases.

#### 5 Experiments

This aim of the research is to investigate the performance and security issues of 802.11b Wireless LANs with multiple clients, hence demonstrating contention in a secure environment. Some of the issues are addressed in this particular paper. How do different security mechanisms affect the performance (delay and throughput) of a congested wireless LAN with multiple clients?

What the effects of different packet lengths on the performance are of wireless LANs using different security mechanisms?

#### 5.2 Design Considerations

There were a few design decisions made before carrying out the experiments. The main three were related to security layers, the traffic generator and the performance measurements used in the experiments. They are described below:

##### Defining Security layers

As part of the research objectives, we wanted to experiment with the effect of WEP authentication and encryption as well as IEEE 802.1x authentication. The security layers, therefore, had to be defined in a way that they would include all the possibilities.

##### Traffic Generator

This research focuses on the performance evaluation of congested wireless LANs. The generator had to be flexible and capable of overloading such networks. The specific requirements we had in mind for choosing a traffic generator were:

- Suitable for wireless networks
- Capable of overloading an 802.11 LAN
- Allowing the user to change the size and inter-packet delay
- Allowing the user to select the generation algorithm

#### 5.3 Measuring performance

Many factors affect network performance and some of them interact to provide overall performance results. Performance results vary depending on the choice of hardware device, software application and network topology [9]. Some of the performance measurements are [10, 11]: Response time, Throughput, Coverage area, Mobility, Bandwidth, Latency, Radio signal strength, etc. Response time and Throughput were measured in this research to provide a comprehensive view of the network performance. They are defined as follows:

- **Response time:** The total time required traffic to travel between two points. It includes the time of dial-up connection establishment, security negotiation time between the server and the clients and the actual data transfer.
- **Throughput:** The total number of bytes transmitted over the network in a given time (response time).

### 5.4 Configuration of Wireless LAN system

It was decided to use Windows-based operating systems, since Windows XP has a built-in implementation of the IEEE 802.1x authentication protocol [12]. As shown in Figure-1 the experiments were conducted using:

#### One Server

- Windows 2003 Advanced server
- 1.4 GHz, 512 MB RAM, D-link DWL 1000+ Access point

#### Two Clients

Windows XP Professional

1.4 GHz, 512 MB RAM, D-link DWL 520+ PCI wireless network card

#### Access Point

- D-link DWL 1000+ Access point

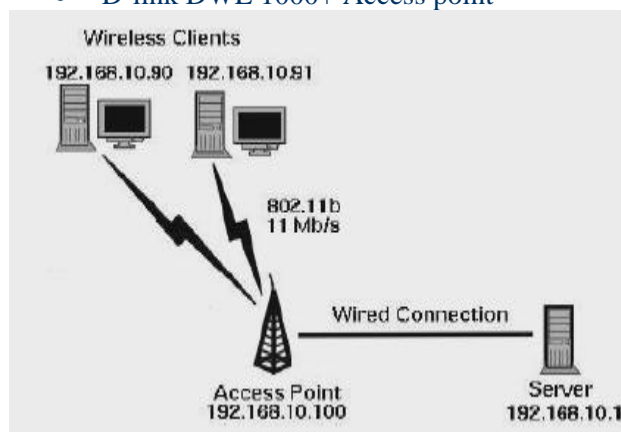


Figure 1: Experimental set up

Transmission speed was 11 Mbps wireless connections between the AP and the clients and 100 Mbps Ethernet connections between the AP and the server. Ethereal [13] Network Analyzer was used to capture live network statistics. The measurements were collected from the server.

### 5.5 Security Layers

The following eight security layers were chosen to present a hierarchical order of the security mechanisms available from both IEEE 802.11 and IEEE 802.1x standards

1. **No security:** this is the default security setting provided by vendors. There is no security mechanism activated with default configuration.
2. **MAC address authentication:** this layer provides MAC address authentication carried out at the AP.

3. **WEP authentication:** the shared key authentication method specified in the 802.11 standard is used.

4. **WEP authentication with 40-bit WEP encryption:** this layer combines the encryption algorithm to provide data privacy.

5. **WEP authentication with 128-bit WEP encryption:** the 128-bit shared key used is proprietary-based (in the case of Lucent).

6. **EAP-TLS authentication:** this is the PKI-based authentication method supported by 802.1x, using digital certificates to authenticate the user.

7. **EAP-TLS with 40-bit WEP encryption:** the combined effect of these tools provides the strongest layer of encryption and authentication using per-session keys.

8. **EAP-TLS with 128-bit WEP encryption:** this layer is the same as above using 128-bit keys.

The first five security layers are consistent with the 802.11 standard. Security layers 6 to 8 are provided by the 802.1x standard.[14]

### 6 Results

The experiments followed the eight security layers described in section 5.5. An infrastructure mode of operation and a single cell were used with two clients. Performance measures were gathered by running five repetitive tests at each security configuration. Experiments evaluating the performance of TCP were separated from UDP's and each set was conducted for different number of clients. Results were collected through log files generated by the Ethereal monitoring tool. Data were analyzed, at the corresponding 95% confidence interval.

#### Effect of security mechanisms on performance

In the first part of the experiments, the bandwidth was set to 500 Kb/s to represent a lightly loaded network (in other words, normal situation when the network is not congested). Figure-2 illustrates the throughput of TCP and UDP traffic types under different security layers, discussed in Section 5.5. These results confirmed the general trends reported in [9], meaning that the stronger the security mechanism implemented, the poorer the network performance.

8), is significantly higher than applying more advanced authentication methods.

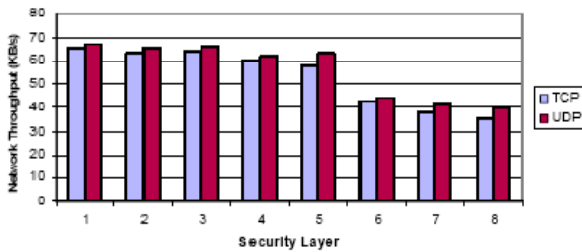


Figure 2 Throughput of TCP, UDP traffic in an unsaturated network

Figure 3 and 4, on the other hand, illustrate the throughput and response times of TCP and UDP traffic types when the network is congested (bandwidth is set to 12 Mb/s).

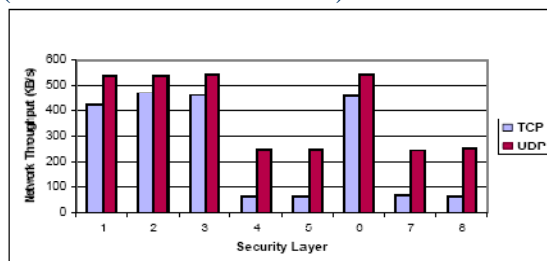


Figure 3 Throughput of TCP, UDP traffic in a congested network

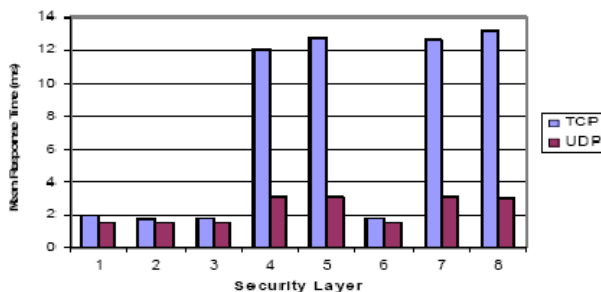


Figure 4 Per-packet response times of TCP, UDP traffic in a congested network

As the graphs show, the performance of a congested network at security layers 4, 5, 7 and 8 (WEP encryption is in place) is significantly less than the performance of the network at security layers 1, 2, 3 and 6. The security layers 4, 5, 7 and 8 decrease the TCP throughput by 85.3% and the UDP throughput by 55.9.3% (on average). In addition, they increase the TCP response time by 84.8% and UDP response time by 52.9%. The results show that in congested networks, the overhead produced by encrypting each individual packet (implemented at security layers 4, 5, 7 and

## Reference

- [1] Karygiannis, T., & L. Owens. (2002). Draft: Wireless Network Security - 802.11, Bluetooth and Handheld Devices. USA. National Institute of Standards and Technology.
- [2] Gast, M. (2002). Chapter 15: 802.11 Network Deployment, 802.11 Wireless Networks: The Definitive Guide. O'Reilly. ISBN 0-596-00183-5. April.
- [3] Xiao, Y., & J. Rosdahl. (2002). *Throughput Limit for IEEE 802.11*. IEEE 802.11 Working Group. May. Document Number: IEEE 802.11-02/291r0.
- [4] Vasana, A., & A. U. Shankar. An Empirical Characterization of Instantaneous Throughput in 802.11b WLANs. Department of Computer Science, University of Maryland.  
<http://www.cs.umd.edu/~shankar/Papers/802-11b-profile-1.pdf>
- [5] Cali, F., M. Conti, & E. Gregori. (1998). IEEE 802.11 wireless LAN: Capacity analysis and protocol enhancement. In Proceedings of INFOCOM.
- [6] Borisov, B., I. Goldberg, & D. Wagner. (2001). Intercepting Mobile Communications: The Insecurity of 802.11. Seventh Annual International Conference on Mobile Computing and Networking. ACM. 16-21 July.
- [7] Amaro, J., & R. P. Lopes. (2001). Performance Analysis of a Wireless MAN. Network Computing and Applications. Page(s): 358-361, 8-10 October.
- [8] Vasana, A., & A. U. Shankar. An Empirical Characterization of Instantaneous Throughput in 802.11b WLANs. Department of Computer Science, University of Maryland.  
<http://www.cs.umd.edu/~shankar/Papers/802-11b-profile-1.pdf>
- [9] Wong, J. (2002). Performance Investigation of Secure 802.11 Wireless LANs: Raising the Security Bar to Which Level? University of Canterbury, Christchurch, NZ.
- [10] Yang, S. J. (2001). An Approach to Modelling Performance Evaluation on the Ethernet with QoS Parameters. International Journal of Network Management, John Wiley & Sons, Ltd. Page(s):91-101.
- [11] Bradner, S., & J. McQuaid. (1999). Benchmarking Methodology for Network Interconnect Devices. RFC 2544. Internet Engineering Task Force. March.
- [12] Microsoft. (2002). Wireless 802.11 Security with Windows XP. Microsoft  
<http://www.microsoft.com/windowsxp/pro/techinfo/administration/wirelesssecurity/XP80211Security.doc>
- [13] <http://www.ethereal.com/>
- [14] Nilufar Baghaei, IEEE 802.11 Wireless LAN Security Performances Using Multiple Clients, Pp-15-35.
- [15] "RealMedia Streaming Performance on an IEEE 802.11b Wireless LAN" Tianbo Kuang Carey Williamson, Department of Computer Science University of Calgary, Pp1-7
- [16] "Performance evaluation of live video streaming service in 802.11b WLAN environment under different load conditions" Yevgeni Koucheryavy, Dmitri Moltchanov, Jarmo Harju Institute of Communication Engineering, Tampere University of Technology, Finland, Pp-1-12