The Second International Conference on Innovations in Information Technology (IIT'05)

Throughput Analysis of WEP Security in Ad Hoc Sensor Networks

Mohammad Saleh and Iyad Al Khatib
iITC
Stockholm, Sweden
{mohsaleh, iyad}@iitc.se

ABSTRACT

This paper presents a performance investigation of the throughput in ad hoc sensor networks. We study the two cases: enabled WEP (Wired Equivalent Privacy), and disabled WEP. The analysis makes use of an ad hoc queuing model with one queue and one server to estimate the security delays in the traffic between ad hoc sensor nodes. We present an algorithm to estimate the service time delay and the security time delay based on real measurements of timestamps. The main result is that the security adds a significant degradation in throughput that may affect applications over ad hoc sensor networks like secure medical application and voice applications.

Keywords: Ad hoc, sensor networks, IEEE802.11b, security, WEP, performance, throughput.

1. INTRODUCTION

Ad hoc networks security is an important need for the success of many applications over sensors network. Security introduces negative effects on the quality of information change by decreasing the throughput. This is due to the reason that security adds more processing and bits to every packet. Many security protocols provide a manageable level to protect the user/customer data over ad hoc sensor networks. We compare the average delay values in two scenarios: (1) when WEP is enabled, and (2) when WEP is disabled. In addition, we look at the effect of the throughput using WEP protocol. Enabling WEP adds more bits to the secured frames and consumes more time processing while decrypting the frames. This increase in processing time and transmission of extra security bits will affect the QoS parameters, which affect throughput, like delay, jitter, and packet loss. Our interest comes from the new IT market, which is witnessing a huge demand on wireless killer applications that are delay-sensitive, like VoIP and other multimedia applications. Quantifying quality is crucial for setting application specific parameters. One goal is to design specific tests and algorithms to quantify the increase in delay due to security. Since the market is moving towards more voice and video applications, we design experiments utilizing User Datagram Protocol (UDP) with varying frame sizes. A mathematical model with one queue and one server can analyze waiting time values, service time values, and throughput. The model makes use of the recorded time stamps of arriving and departing packets. A key result is a mathematical model for the analysis of WEP security performance. Our results show that WEP security adds a significant delay that decreases the throughput monotonically. Using our queuing model, the algorithm can estimate the extra microseconds needed for security, which drastically affect the throughput. This research evaluates performance of network throughput in order to set application parameters to enhance QoS.

2. AD HOC THROUGHPUT QUEUING MODEL

Representing ad hoc throughput sensor networks with queuing models assumes a queuing system for each ad hoc sensor node. Each queuing system consists of one queue and one server. This model measures the throughput for several scenarios using dissimilar security protocols implemented over ad hoc sensors networks. Our ad hoc throughput queuing model can also improve performance via the use of a new parameter, which we introduce as the ***quality figure of merit*** or QFoM in our coming

paper (Figure1). The QFoM includes many parameters like throughput, number of users, noise effect parameter, and protocol dependent index, which are the subject of our ongoing research, and we do not discuss them on this paper. However, the results of this paper are the initial step that intrigued us to start on the QFoM.

Figure 2 demonstrates the mathematical model. The algorithm defines the process from the time that transmitted data enters the wireless part of the source node until it reaches the destination node and then enters the Network Interface Card (NIC) using the following steps:

1- Register the time data transmitted by recording the timestamp of the packet after all bits have entered the queue.
2- Data entering the queue waits until it enters the service facility (server).
3- Data entering the service facility will get encapsulated in an IEEE802.11b MAC frame, which is also encapsulated in the Physical Layer Convergence Protocol (PLCP) header and preamble. In addition, the security headers are added or removed in the server by enabling or disabling WEP protocol as shown in Figure3 [1].

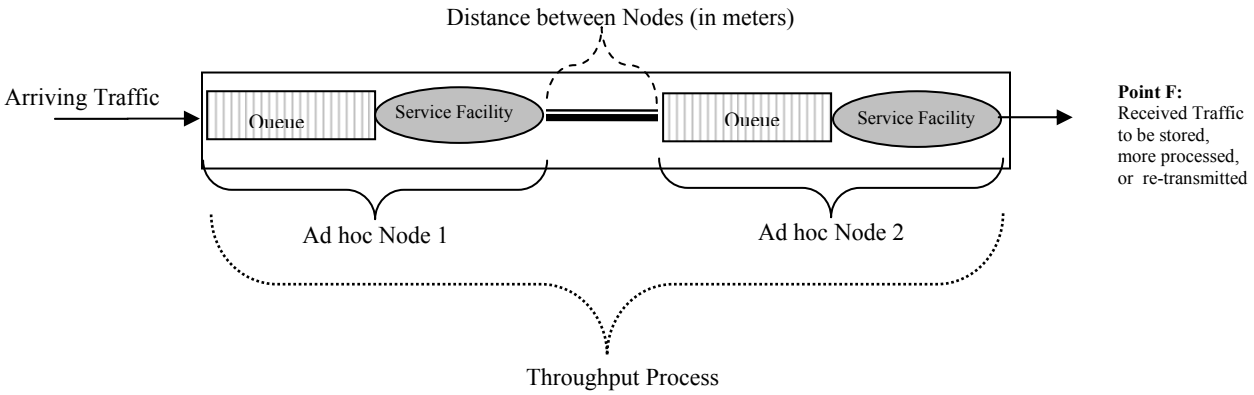

Figure1. Ad hoc throughput queuing model with two sensor nodes

4- Throughput measurements process depends on the number of packets transmitted with or without WEP over the transmission speed of 11Mbps and the physical distance in meters.

Using ad hoc systems and our ad hoc queuing model, we are able to define the total time, service times, packet lost, and throughput, for the arriving traffic (packets) that are to transmitted between ad hoc sensors and throughput.

3. AD HOC THROUHGPUT QUEUING MODEL ALGORITHM

The throughput queuing algorithm depends on the following factors according to our experiments: service time, queuing time, and the distance between sensor nodes. The delay in each node consists of two major parts: (1) the waiting time in the queue, and (2) the service time. The summation of these two is equal to the response time of the sensor node. The waiting time is defined as the time needed for a packet to wait in the queue before it is served and the service time is defined as the time

from when a packet leaves the queue and enters the server until it departs from the last node server. Hence, the service time, waiting time and response time are as follows:

Response time (Rt) = Departure time (Td) – Arrival time (Ta) = Waiting-time (Wt) + Service-time(St) (1)

and the throughput is defined as:

Throughput = Number of IP data bytes (without IP header bytes) received at the final point (Point F) in the final node (2)

Total time from the first traffic arrival till all data is at the final sensor node

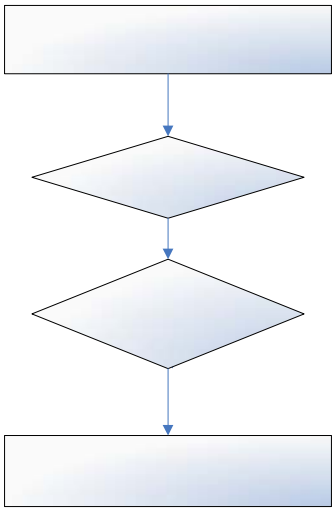

Figure2: Ad Hoc Throughput algorithm

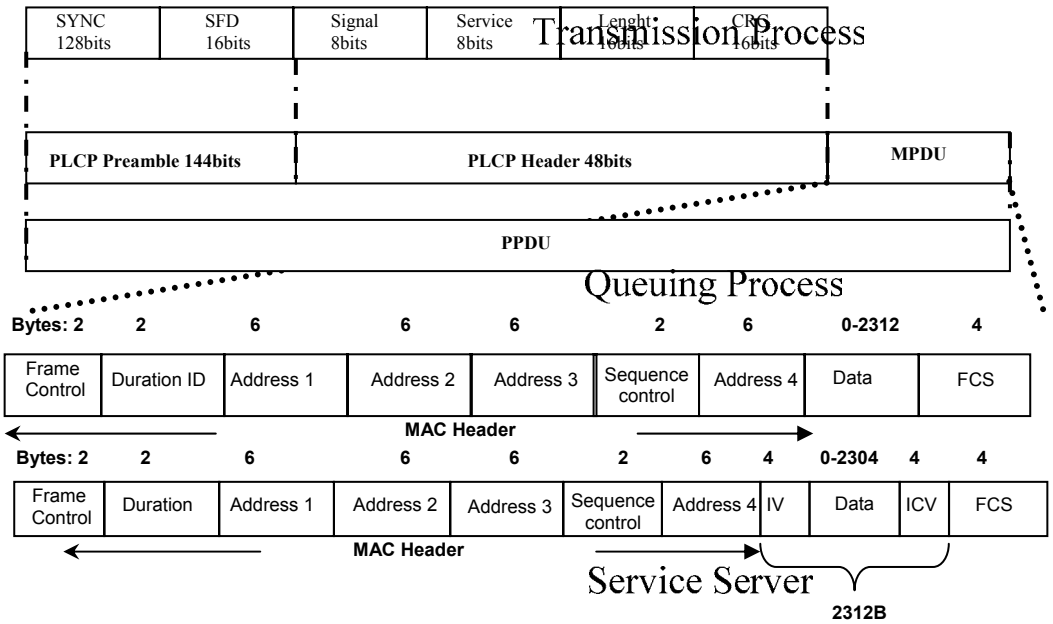

Figure 3: IEEE802.11b frame format. The MPDU is the MAC Protocol Data Unit, which expanded in the last shown frames.

Throughput Measurement

4. EXPERIMENTS

The experiment test-bed consists of two laptops with Linux kernel 2.4.27 operating system and Lucent Orinoco IEEE802.11b wireless cards set on ad hoc mode. The traffic generated between the ad hoc sensor nodes uses UDP to avoid feedback Acknowledgement (ACK) packets that TCP adds.

To solve the problem of timing synchronizations, the ad hoc nodes are synchronized via a local server to which all test-bed nodes are connected. The same test is repeated several times (at least three times per test) with *network STUMBLER* version 4 to measure the noise environments. The steps performed during the experiment are described below:

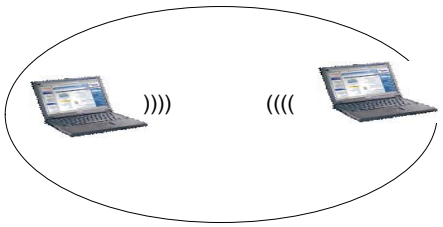

Figure 4: Ad Hoc mode.

1- *Security test:* in this step of the experiment, WEP security shared key was set ON between the ad hoc stations with 40 bit encryption keys. The UDP payload starts at 32B and is incremented by 32B until the maximum data limit that can be sent over IEEE802.11b with WEP, which is 2304B (see Table 1). Table 1 and Table 2 show a difference between the maximum number of bytes we can send when WEP is enabled and when WEP is disabled, because thee are 8 bytes increase in the payload as shown in Figure 3. The number of packets sent between the ad hoc nodes is calculated according to (3), (4) and (5) [2] [3][4]:

Frame Size (bits) = DIFS + PLCP + MAC-header + FCS + WEP + IP-packet + SIFS +ACK + Back off (3)

(IP-header + UDP-header + UDP-payload)

Number of packet per second = Utilized bit rate / Packet Size In bits (4)

Theoretical Max. Throughput = $\frac{\text{UDP-payload} * 8 * 1000000}{\text{PLCP\_time}+(\text{IP} * 8 /R)+\text{SIFS}+\text{PLCP\_time}+(\text{ACK} * 8 / R)+\text{DIFS}+(\text{Backoff} / 2) * \text{Slot}+(\text{WEP}*8)/R}$ (5)

where, [1]

- DIFS = 50µs
- PLCP header = 192 bits
- MAC header and FCS = 34 bytes
- WEP = 8 bytes

- IP packet = 20 bytes + UDP header + UDP payload variable
- SIFS =10μs
- ACK = 304 bits
- Back off = 20μs.

Table1: UDP payload packets sent between ad hoc nodes with WEP encryption

UDP payload (Bytes)	Packet Size Bits	Number of Packet per Seconds
32	2234	5160
128	3002	3840
512	6074	1900
1024	10170	1130
2284	20250	569

2- *No Security test*: in this step of the experiment, WEP security is put OFF between the ad hoc stations, and the UDP payload was initiated from 32B and incremented by 32B till the maximum data could be transferred over IEEE802.11b without security. The maximum amount was 2312B (see Table 2). The number of packets sent between the nodes is calculated according to (3), (4), and (5).

Table 2: UDP payload sent between ad hoc nodes without WEP encryption.

UDP payload (Bytes)	Packet Size (Bits)	Number of Packet per Second
32	2234	5160
128	3002	3840
512	6074	1900
1024	10170	1130
2269	20130	572

5. RESULTS

Our results are for two categories of throughput: (I) with WEP and (II) without WEP. The practical experiment analyses show that, within the same category (within category I or within category II), as the payload increases the throughput increases and then decreases, which is a very interesting results. Another key result is that for the same packet size, the throughput is relatively higher than when WEP is enabled. However, the difference in throughput between category I and category II is not so large. Moreover, degradation in the QoS is a function of the number of attached users, the distances between them, and packet sizes of each user stream. Table 3 and table 4 show the results of throughput values, which can be used to feed applications of the network performance in order to enhance application performance.

Table 3: Throughput for IEEE802.11b without WEP encryption

UDP payload (Bytes)	Average throughput for IEEE802.11b without WEP encryption(Mbps)
32	0.26
128	0.52
512	0.27
1024	0.25

Table 4: Throughput for IEEE802.11b with WEP encryption

UDP payload (Bytes)	Average Throughput for IEEE802.11b with WEP encryption(Mbps)
32	0.62
128	0.77
512	0.54
1024	0.54

Performance degradation for ad hoc Wireless Sensor Networks of IEEE802.11b using WEP occurs because the WEP header has an initial vector and an Integrity Check Value (ICV) [1]. This header is augmented to the packet before transmission. Moreover, the RC4 security algorithm [1] generates the stream key and runs its XOR operation with the IP payload. The increase in the packet size increases time consumption. The decryption on the ad hoc destination introduces a higher delay. The extra security bits and the XOR-related time delays lead to throughput degradation [5].

CONCLUSION

We present a queuing model and algorithm to analyze the throughput of ad hoc sensor networks for two categories: with WEP and without WEP. We analyze the throughput between the sensor nodes of IEEE802.11b. A comparison study shows that the performance is degraded when WEP is enabled compared to when WEP is disabled, but the degradation is not so large. However, a key result is that the throughput is affected by packet size and this affects delay-sensitive applications like VoIP and video streaming. As the packet size increases, the throughput increases till some packet size value (around 128B UDP payload) and then the throughput decreases. The distance between sensors nodes has an effect on the throughput. A key result is that the difference between the throughput of WEP experiments and the standard mode for the same payload is a function of the packet size. Therefore, QoS degradation is a function of the number of attached users and packet sizes of each user stream. The proposed ad hoc throughput queuing model and its related algorithm can be implemented in ad hoc sensor networks to better the performance of real time applications especially VoIP, by distributing traffic and location for sensors network and by choosing more suitable packet sizes.

REFERENCES

[1] IEEE Std 802.11-1997, "Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications".
[2] Matthew Gast, "802.11 Wireless Network The Definitive Guide," 1st Edition, 2002.
[3] William Stallings, "wireless communication and networking," prentice Hall,2003.
[4] Cisco 7920 Wireless IP Phone Design and Deployment Guide, March 2005.
[5] Mohammad Saleh and Iyad Al Khatib, "Wireless Access Point Security Performance Using WEP Encryption," ACM MobiSys 05 The Third International Conference on Mobile Systems, Applications, and Services, June 6-8, 2005, Seattle, Washington, USA.