Effects of Security Features on the Performance of Voice Over WLAN

Changhua He
Electrical Engineering
Stanford University
changhua@stanford.edu

Abstract:

This project studies the effects of security features on the per packet delay and loss rate of voice traffic over WLAN. We model the security features by adding packets and extending the length of each data packets. Different authentication and encryption schemes (WEP with Challenge-Response authentication and TKIP with a long term shared key and 4-way handshake) are investigated to represent the common secure WLAN implementations. Based on our simulation, when the traffic load is light in the network, adding security features does not decrease the performance, while the network performance will decrease more rapidly when the traffic load is getting higher and higher. That is because in 802.11 MAC, the frame body is transmitted in a higher rate (11Mbps) than the packet overhead, the number of packets transmitted over 802.11MAC dominates the performance in this case, instead of the length of the packets.

1. Introduction

Nowadays Wireless Local Area Networks (WLAN) has been deployed more and more popularly. It provides much more flexibility than the wired for networking scenarios such as college campus, coffee shop, airport and so on. Also due to the much higher transmission rate comparing to current cellular systems, it is considered to be possibly the main component of the next 4G systems, or at least part of it.

On the other hand, Voice over the Internet Protocol (VoIP) technology has been well developed and implemented in wired networks widely. The motivation of VoIP is the low cost to transmit voice over Internet, especially for long-distance calls. Generally a VoIP application consists of the codecs (Coder-decoder), the Real-Time Protocol (RTP), the Real-Time Control Protocol (RTCP) and the User Datagram Protocol (UDP). The codec is usually a Digital Signal Processor based system employing one of the compression algorithms, the RTP is an IP-based protocol providing support for transporting real-time data such as video and audio streams. In an RTP session, participants periodically send RTCP packets to convey feedback on quality of data delivery and information of membership. UDP is the transport layer chosen to send the packets over IP-based network without guarantee.

From the success of VoIP, together with the wide deployment of WLAN, a general but useful idea is to transmit voice over IP over WLAN, where WLAN (802.11b and so on) is implemented as the MAC and PHY layer. Voice over WLAN has really captured the imaginations of enterprise users, or vendors for that matter. This promises significant cost savings on moves, adds and changes, very sophisticated user-programmable customization features. Furthermore IT personnel may only support one common network infrastructure.

Many works have been done to study the performance of transmitting voice over WLAN. In [1] Hole and Tobagi give out the analysis and simulation results of the capacity of VoIP over WLAN under different codecs, varying delay constraints, channel conditions and voice call quality requirements. Many other related researches are also done in the literature [2, 3, 4, 5, 6, 7]. However, none of them consider the security features, which are very important requirements to implement such a system. Nilufar Baghaei [8] studies the performance of Wireless 802.11 networks under different security levels, but his study is based on measurement of a real WLAN system which consists of several stations and one AP. Obviously this is highly product-related and can not disclose the characteristics of WLAN under different security levels with many stations present. Also the author does not consider the special requirement of the voice traffic, in which delay and loss are the most important issues.

In this project, we are trying to simulate and analyze the performance of voice traffic over WLAN under different security levels. Note that we won't touch the physical characteristics of the wireless links, instead, we will focus on how the quality of the voice traffic, say, the packet delay and loss rate, is affected by the security mechanisms. For each security mechanism, the influence on the performance lies in both the per packet encryption/decryption delay and the extra packets and extended packet length. In this report we only consider the influence of extra packets and extended packet length imposed by the security features. More discussions on encryption/decryption delay can be found in Section 5.

The report is organized as follows. Section 2 introduces the different security schemes and describes our method to model them for comparison. Section 3 describes our simulation strategy and setups. Sections 4 shows the simulation result and analysis based on comparison of VoWLAN without security implementation and the similar systems with security improvements. Section 5 gives out more discussions to explain the result difference from [8]. Section 6 concludes our work.

2. Security Models

Security is a serious concern in WLAN system because the wireless medium is open for public access within a certain range. There are many requirements for security in real world, each representing some specific features. Obviously for voice traffic, authentication and data encryption are the most important issues that users care about. Authentication can make sure that a valid user, instead of a malicious one, is consuming

resources in the AP to access the network. Also it can assure a user is talking to somebody that supposed to be, not anybody else. Data encryption provides secrecy to the content of the ongoing transmissions. Nobody except the valid parties involving in the communication can understand, generate or modify the valid messages.

2.1 Security Models

At first, Wired Equivalent Protocol (WEP) is proposed [9] to encrypt the data stream and provide a poor authentication. Soon it is found to be completely unsafe. Upon this Wi-Fi Alliance proposed Temporary Key Integration Protocol (TKIP) for fast re-keying to improve the secrecy. Furthermore an authentication protocol based on 802.1x [10] is developed to take place of the poor open system authentication and WEP authentication. Currently the latest IEEE std. 802.11i is approved to support stronger authentication and data secrecy. But the user need upgrade their hardware in order to implement the complete protection by 802.11i.

In this report, we will consider the effects of both authentication and encryption schemes. We will compare three kinds of VoWLAN system. The first one is implemented without any security considerations, the second uses a simple Challenge-Response scheme for authentication and WEP for data encryption, the last one implements the strongest security by 802.1x [10] based authentication and TKIP for data encryption. However, we won't cover the complete implementation of 802.11i. The reason lies on two facts. First, 802.11i suggests an authentication scheme that is also based on 802.1x. Second, 802.11i defines a new data encryption algorithm based on Advanced Encryption Standard (AES), which need hardware upgrades on the current devices, and is not implemented in any products up to now.

We will use NS2 to simulate the network, but it is well known that NS2 doesn't implement any security features. We won't implement the security things in NS2 either, because security is a subtle thing related to many aspects, which is much different from other kinds of network protocols. Instead, we only want to model the process of the security features and explore their influence on the voice performance.

Both the authentication and encryption will influence the performance of the system. For authentication, it will add some extra time on setting up the call at the beginning, also it will influence the performance by adding more traffic into the network for the authentication handshake. On the other hand, for data encryption, it does not add any extra message into the network, but it has influence on the performance due to the encryption/decryption delay and the increasing size per packet. In this study we do not consider the encryption/decryption delay, instead we will discuss their effect in Section 5.

2.2 WEP security

In WEP two weak authentications are defined, in addition to a general MAC address filtering implementation. One is Open System authentication based on BSSID, the other is a Challenge-Response process. We will focus on the Challenge-Response approach though it still provides poor authentications. The authentication process is described in Figure 1 as follows.

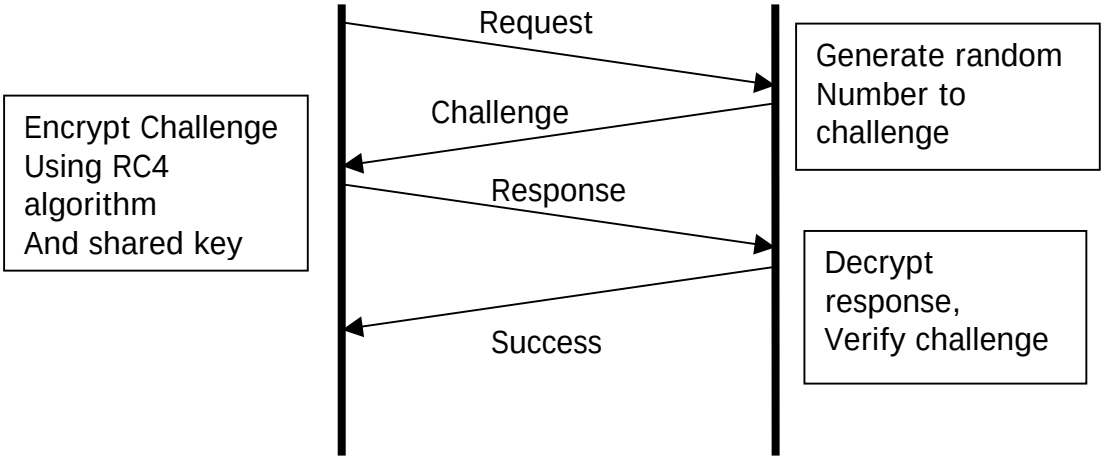

Figure 1. Challenge-Response Authentication Process

As we can see, this authentication imposes 4 messages for the handshake. Furthermore, WEP adopts an encryption algorithm based on RC4, which encipher the data streams based on a shared key. It works as shown in Figure 2.

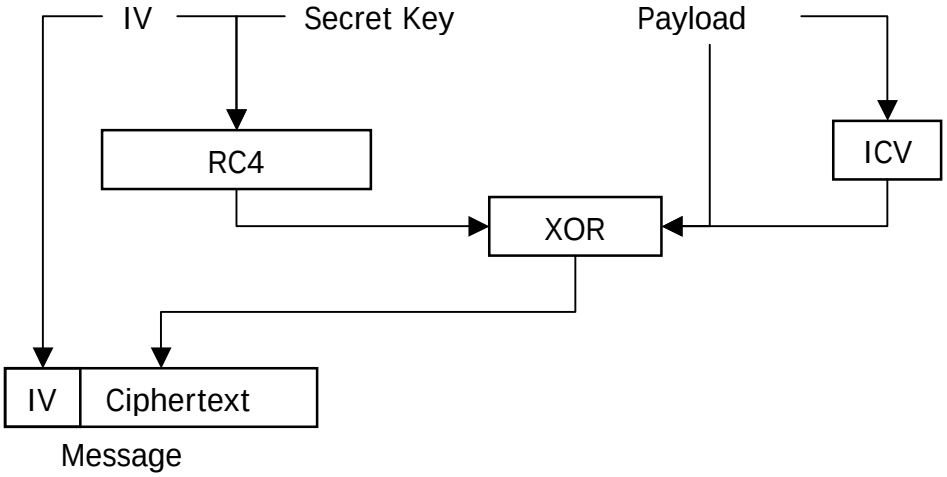

Figure 2. WEP encryption process

Because the destination station only knows the shared key but has no idea on the Initial Value. The encrypted packet should be transmitted together with the 4-Byte IV, furthermore, a 4-Byte Checksum value is attached to prevent malicious modifications.

2.3 TKIP security with 4-way handshake

In 802.1x authentication, many rounds of message exchange should be done to set up a shared secret between the AP and the station, in general that will be intolerant for a real time communication. The approach to deal with this is to use a pre-shared key or re-use one key for a relatively long period, although this will decrease the security. In this senario, the station and AP also need to do a 4-way handshake to confirm the shared key and derive a temporary session key, as shown in Figure 3. We only consider this as the extra overhead introduced by the authentication process. Note that this handshake is defined in the latest 802.11i standards.

Message 1 (A->S):
AA, ANonce, Sequence(n), msg1
Message 2 (S->A):
SPA, SNonce, Sequence(n), msg2, MIC_{PTK}{SNonce, Sequence(n), msg2}
Message 3 (A->S):
AA, ANonce, Sequence(n+1), msg3, MIC_{PTK}(ANonce, Sequence(n+1), msg3}
Message 4 (S->A):
SPA, Sequence(n+1), msg4, MIC_{PTK}{Sequence(n+1), msg4}

Figure 3. 4-way handshake process

In Figure 3, S represents the station and A represents the Access Point; SPA and AA, SNonce and ANonce represent the MAC address and nonces of the station and access point respectively; msg1, 2, 3, 4 are indicators of different message type; PTK (Pair-wise Temporary Key) is calculated from PRF-X(PMK, "Pairwise key expansion", AA||SPA||ANonce||SNonce) and divided into KCK (Key Confirmation Key), KEK (Key Encryption Key) and TK (Temporary Key); MIC_{PTK}{…} represents the MIC (Message Integrity Code) calculated for the content {…} with the PTK. Note that actually MIC is calculated with KCK, which is only part of PTK, however, we won't distinguish them here because there are no confusions for the authentication process. Also note that in the original protocols, RSN IE fields are included in Message 2 and Message 3 to negotiate cipher suites, and encrypted GTK are sent in Message 3 in multicast applications.

Obviously this authentication also imposes 4 messages per call. Beyond that, TKIP defines the data encryption based on RC4 as well as in WEP, but use a larger IV space and faster re-keying to improve the security, and implement a Message Integrity Code (MIC) which is much stronger than the checksum approach in WEP. The encryption process is shown in Figure 4.

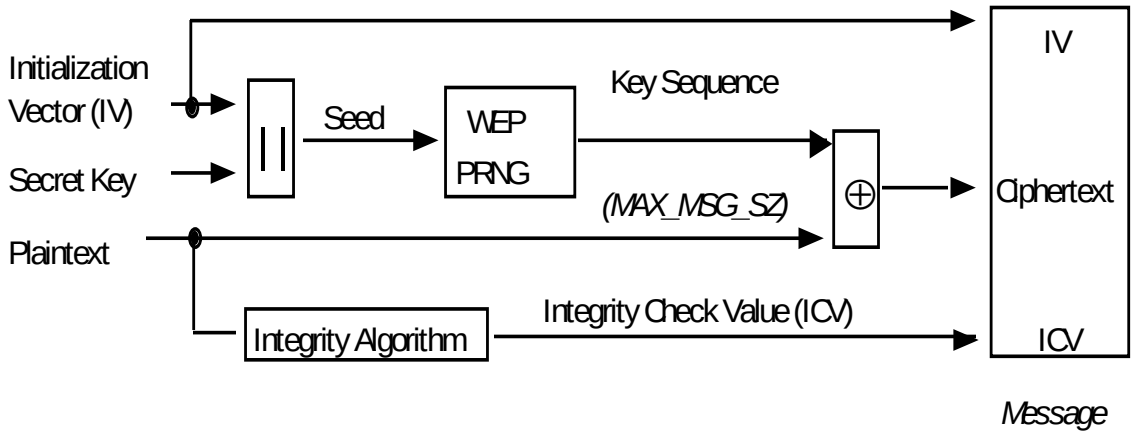

Figure 4. TKIP encryption process

After the encryption, the message is extended with 4 more bytes Extended IV and 8 more bytes MIC comparing to WEP, the actual component and size of the packet is shown in Figure 5 as follows.

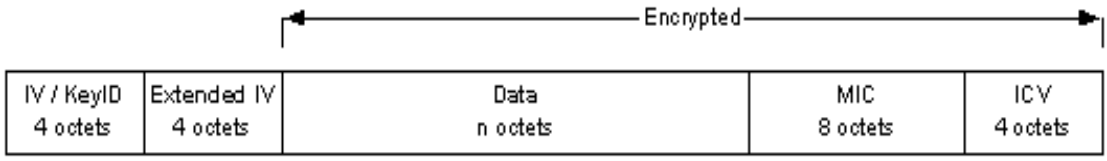

Figure 5. TKIP data packets

In this report, we will consider the effects of each security scheme on the voice performance lie on two facts. First, the extended packet size will introduce more transmission, thus more delay. Second, the messages for authentication will introduce extra traffic into the network, thus increase the probability of collision or packet delay. We won't consider the increasing call set up time because generally the user can tolerate a longer call set up in the extent of seconds, which is much longer than the delay caused by the network (should be in the extent of ms).

3. Simulation Setups

In this simulation, we use Network Simulator 2 (NS2-2.27) to simulate the behavior of 802.11b networks. The following scenarios are constructed as shown in Figure 6. All stations are randomly located in the transmitting range of each other (200x200), each station will request a connection to the AP at random start time. Based on this scenario we will consider two traffic configurations. For configuration 1, each station will set up a call, then continue to send out voice packets until the simulation is terminated. For configuration 2, each station will set up a call, send packets for some time, terminate the

call, then set up another call again, and so on. Through these two configurations, we want to study the effects of data encryption and authentication respectively.

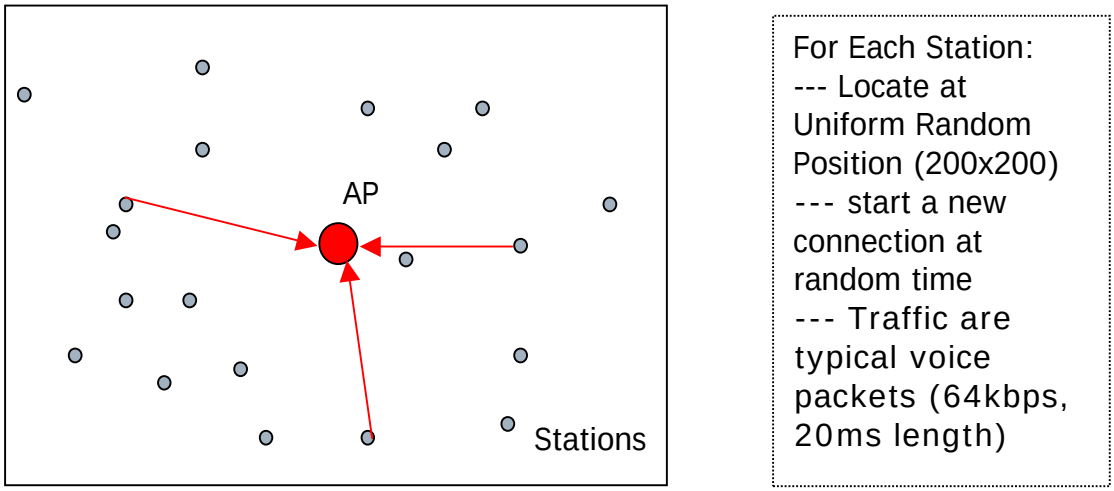

Figure 6. Simulation Scenarios

The following flow chart in Figure 7 illustrates our simulation process. For each configuration described above, we run some C program to generate the input trace files from none security scheme, WEP scheme and TKIP scheme separately, then use NS2 to simulate the network behavior for these input trace files. Based on the output trace file, we calculate the average per-packet delay, average drop rate and compare them in these three schemes.

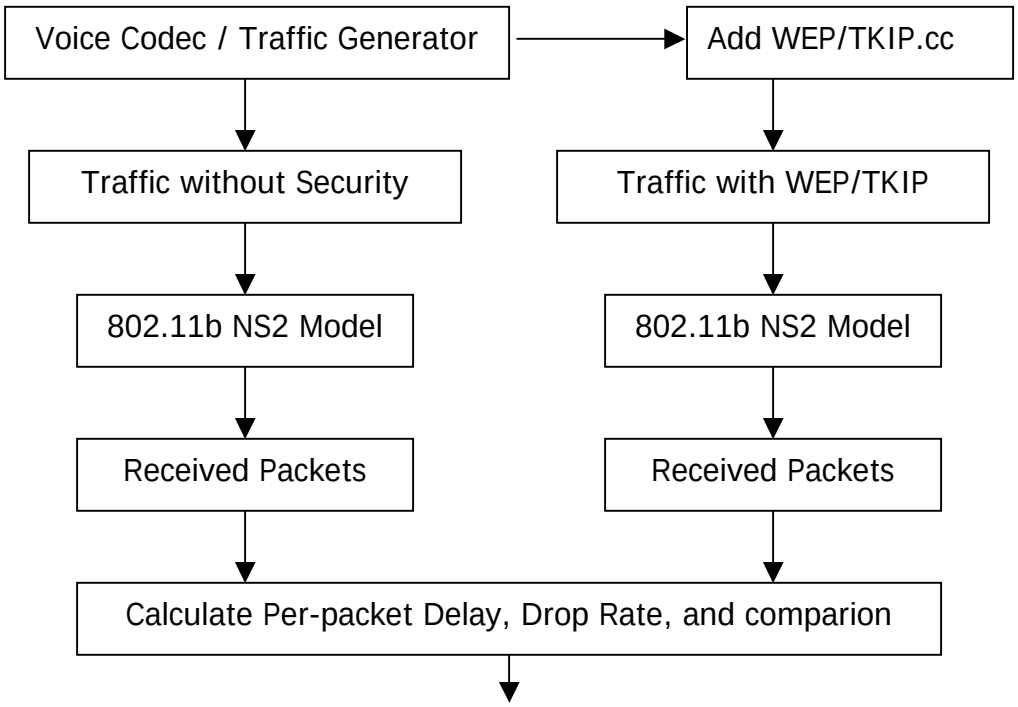

Figure 7. Simulation Configurations

4. Results and Analysis

As we discussed above, we will only consider the effects of extra packets or extended packet length imposed by the security schemes. There are two kinds of such packets, one comes from the encryption process (extended length), the other comes from the authentication process, in which a number of extra packets are included at the beginning of each call. In order to make clear how they affect the voice performance, we will user two different configurations to explore them separately.

4.1 Long Duration Calls

This configuration is used to test how the encryption overhead (extended packet length) affect the delay and drop rate. In this simulation, each station set up a call to the AP at random starting point, then continue to send out packets until the simulation ends. The calculation of per-packet delay and drop rate is done only for the data packets sent out after a specific period, say, all the stations have set up the connections.

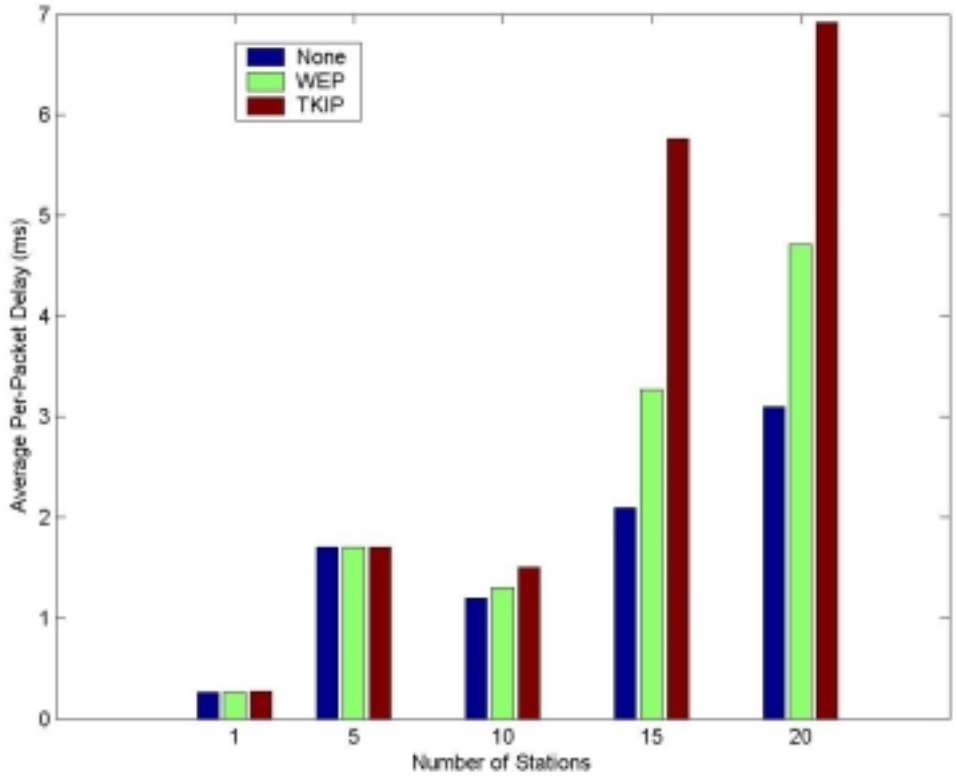

Figure 8. Per Packet Delay for long duration calls

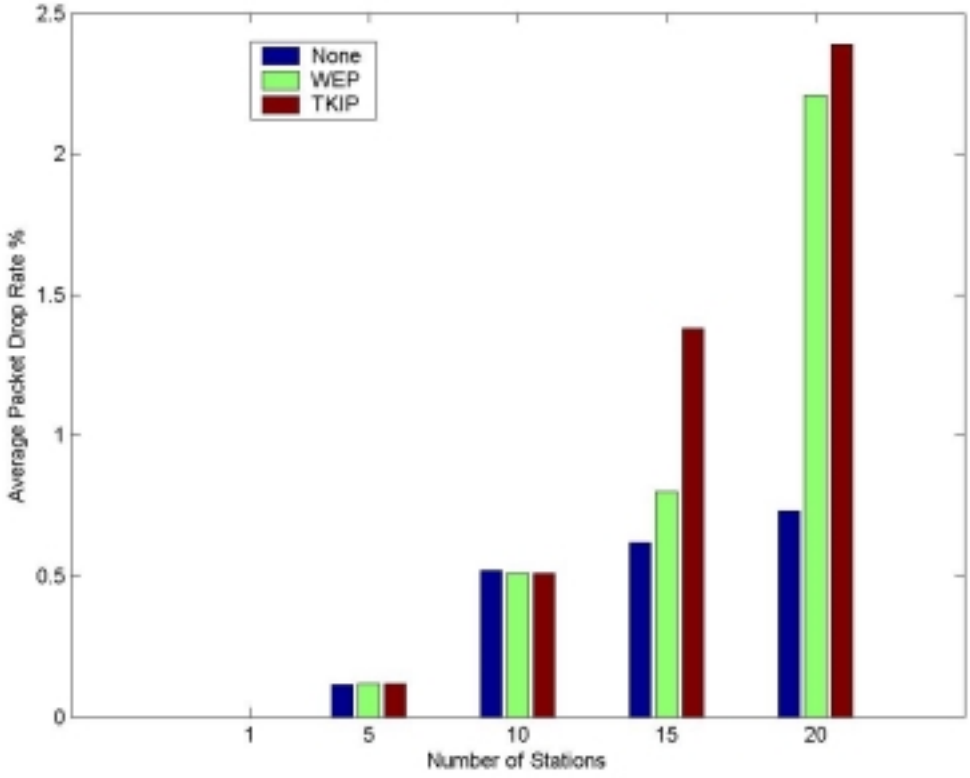

Figure 9. Drop Rate for long duration calls

From Figure 8 and 9, we can see when the number of stations is small (say, less than 10), adding security features, no matter WEP or TKIP, does not influence the voice performance. However, when the network is getting more and more crowded (say, more than 15 stations), adding security features will increase the packet delay and drop rate rapidly, thus decrease the voice performance. For example, for 1 or 5 stations, there are no difference for the three schemes in packet delay and drop rate. For 10 stations, packet delay will increase a little when adding security features, but drop rate almost keep the same. However, for 15 and 20 stations, both packet delay and drop rate increases rapidly when adding any security features. Furthermore, we can see generally TKIP is worse than WEP due to its larger packet size.

4.2 Short Duration Calls

From the simulation in Section 4.1, we have known the effects of encryption scheme by extending the packet length. In this section the configuration is used to explore the effects of the authentication process. Each station will set up a new call to the AP at random starting time, continue to send out packets for a period of duration (5s), then close the connection and set up a new call to the AP again, and so on. The results are shown in Figure 10 and 11.

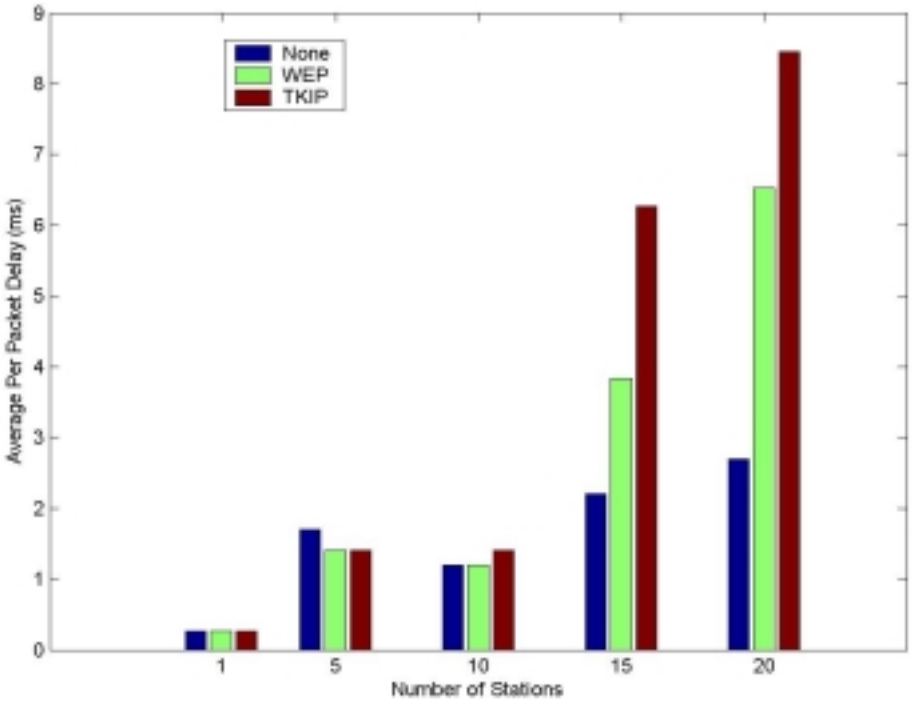

Figure 10. Per Packet Delay for short calls

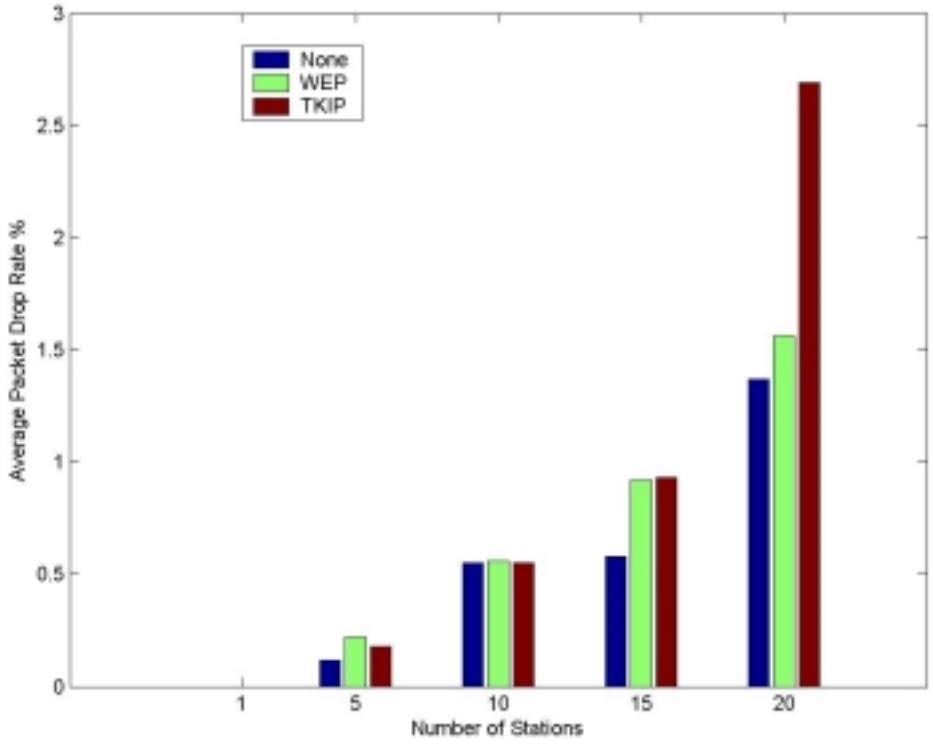

Figure 11. Drop Rate for short calls

Similarly as in Section 4.1, we see that when the number of stations is low in the network, adding security does not decrease the performance of the network. But when the number of stations increases, adding security features will decrease the voice performance more and more rapidly. Also another observation is that, even we adopt a quite short call time (5s), which is not so applicable in real world, the effects on the performance under light traffic is nearly not perceptible. That is because even within 5s, there will be 250 data packets, which is much larger than the authentication packets (4 for each call). Though the authentication packets is larger than the data packets, the data packets will dominate the transmitting process because the number of packets is more important than the packet size, due to the large overhead per packet imposed by the 802.11b MAC mechanism.

5. Discussions

From above sections, we have concluded that when the number of stations is low in the network, the security features do not affect the voice performance very much. However when the number of stations is getting higher, adding security features will increase the per-packet delay rapidly.

We have done more simulations to study the effects of adding security features. First we change the data packet size from 160 bytes (corresponding to 20 ms interval) to 80 bytes (corresponding to 10 ms interval), this does not change our result very much because the data packets are transmitted at very high speed (11Mbps), while the preamble and other additional information are transmitted at relatively low speed (1Mbps). This is also the reason why extending the packet size in each security scheme does not affect the performance very much.

Second, for configuration 2 in section 4.2, we change the average call duration from 5s to different values (10s and so on), similarly that doesn't change our observations. Basically when the traffic load is not so high, the most important fact that affects the network performance is the number of packets transmitted in the network, not the size of the packets, because the performance is dominated by the overhead in 802.11 MAC. We omit the details in section 4 because all the results are similar to those in Section 4.1 and 4.2.

Furthermore, we can see the per-packet delay are relatively small comparing with the result from [8], say, in the extent of less than 10 ms, while in [8], the network performance decreases greatly with only several clients in the system through measurements. The possible reason is that other properties we ignored in this simulation affect the performance more than the packet size extension and the authentication packets. Specifically, in a real wireless card, the encryption/decryption time will impose a significant delay to each packet if the computation power is not strong enough, that is the real situation that we do not consider in our simulations. But because this kind of delay caused by encryption/decryption relates highly to the hardware, the packet size and the instantaneous computation load on the device, it is hard to model them accurately, maybe this can be a future work for the extension of this project.

6. Conclusion

In this project, we study the effects of different security features on the performance of voice traffic over WLAN, specifically we compare the performance of none security, WEP implementation and TKIP implementation. In each security scheme, both authentication and encryption are taken into account. And we focus on the effects of extra packets and extended packet length imposed by the security schemes.

Based on our simulation and analysis, in case that the traffic load is light in the network, adding security features does not decrease the packet delay and packet loss rate, while in case that the traffic load is high, the security features will decrease the network performance more rapidly. Also due to the characteristics of 802.11 MAC, the more important fact that influence the performance is the number of packets transmitted by the MAC layer, not the length of each packet. In practice, the encryption/decryption delay also affect the performance in a significant way because of the limited computation power.

References:

[1] David P. Hole and Fouad A. Tobagi, "Capacity of an IEEE 802.11b Wireless LAN supporting VoIP", to appear in Proc. IEEE Conference on Communications (ICC) 2004.
[2] A. Kopsel and A. Wolisz, "Voice transmission in an IEEE802.11 Wireless Local Area Networks", IEEE Communications Magazine, September 1997.
[3] S. Garg and M. Kappes, "An experimental study of throughput for UDP and VoIP traffic in IEEE 802.11b networks", IEEE wireless Communications and Networking 2003.
[4] Xiao, Y., J. Rosdahl, throughput limit for IEEE 802.11, IEEE 802.11 working group, may 2002, Document number: IEEE802.11-02/291r0.
[5] Bing B., "Measured performance of the IEEE 802.11 wireless LAN", Local Computer Networks, LCN'99. Pages 34-42, 18-20 October, 1999.
[6] Chandran-Wadia L., S. Mahajan, S. Iyer, "Throughput Performance of the Distributed and Point Coordination Functions of an IEEE 802.11 Wireless LAN".
[7] IKKurthy P., M. A. Labrador, "Characterization of MPEG-4 traffic over IEEE 802.11b wireless LANs", Local Computer Networks, LCN'02, Pages 421-427, 6-8 November, 2002.
[8] Nilufar Baghaei, "IEEE 802.11 Wireless LAN Security Performance Using Multiple Clients", Honors Project Report, 2003
[9] IEEE Std. 802.11b (1999), Supplement to ANSI/IEEE Std. 802.11, 1999 Edition, Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications: Higher Speed Physical Layer (PHY) Extension in the 2.4 GHz band. IEEE, Inc. ISBN 0-7381-1811-7, September 1999.
[10] IEEE Std. 802.1x (2001), Port-Based Network Access Control, New York, IEEE, Inc. ISBN 0-7381-2627-5, 25 October 2001.