LAP: Link-Aware Protection for Improving Performance of Loss and Delay Sensitive Applications in Wireless LANs

Avesh K. Agarwal Wenye Wang Rachana A. Gupta Mo-Yuen Chow
Department of Electrical and Computer Engineering
North Carolina State University, Raleigh, NC 27695

Abstract - Radio links exhibit highly unpredictable properties such as variable bandwidth and bit error rates that affect the performance of applications in wireless networks. Besides, another critical concern is the protection of applications due to shared and open wireless medium. However, protection services add additional performance overhead to carry out their operations, and incur varying effects on the network performance, depending on link characteristics. Thus, how to provide protected and high performance service is a challenging issue in wireless networks. The problem is even more challenging for real-time applications such as voice over IP (VoIP) with stringent delay and packet loss requirements. In this paper, we present a novel approach to improve application performance by implementing Link Aware Protection (LAP) in wireless local area networks (LANs). LAP exploits dynamic security policy management (DSPM) scheme for adapting protection with varying link quality. We present a real-time implementation of LAP in our wireless LAN test-bed. As a case study, we demonstrate VoIP performance on our LAP enabled wireless clients. The results show the possibility of maintaining an adequate protection and achieving improved performance for VoIP streams under link variations.

Keywords- Wireless LANs, dynamic protection, performance, voice over IP.

I. Introduction

The popularity of wireless LANs as hot spots has been increasing in the recent years. In addition to email and web-surfing, application trend is moving towards real-time applications such as voice over IP (VoIP) and video [20]. However, the unfriendly medium characteristics of wireless networks impose serious challenges in realizing stringent quality of service (QoS) requirements of real-time applications such as VoIP in wireless LANs. For example, wireless medium exhibits unpredictable and rapidly changing error characteristics which lead to high packet losses [18]. Also, wireless medium being a shared medium leads to frequent packet collisions, which in turn, cause packet losses and delay in the networks. Moreover, wireless medium is prone to attacks by malicious users [17], [11], [26]. Consequently, protection is of paramount importance in wireless LANs, and requires the use of protection services to counteract the potential attacks.

However, protection services add extra overhead in the network for carrying out their operations. The protection services add two types of overheads - additional headers/ trailers, and extra processing delay for encryption/decryption, hashing, and adding headers/trailers, etc. Additional headers and trailers increase the packet size of applications running in the network. The increased packet size and extra delay lead to higher probability of packer errors and collisions, which in turn, cause higher packet losses and high jitter in application traffic. Since real-time applications are highly sensitive to packet losses, delay and delay jitter, it becomes a critical concern to achieve desired performance of these applications with protection services. Therefore, we observe that there exists a conflict between performance and protection to transmit real-time applications reliably in wireless LANs.

Our focus in this paper is to deal with the interdependence of protection and performance of VoIP. The primary reasons to focus on the protection are many folds. First, we believe that the protection is the most important and integral service required for wireless LANs with open medium. Thus, it becomes imperative to evaluate the performance of VoIP in a wireless LAN with protection services. Second, previous studies have not discussed improving VoIP performance by considering protection as the main factor. It creates a gap in dealing with better performance and better protection for real-time applications in wireless LANs. Therefore, our effort is to fill the gap which will ensure required VoIP performance under adequate protection in wireless LANs. The problem becomes even more important in military wireless networks, in which applications, such as voice and video, require protection with better performance.

We present a novel approach to improve performance of VoIP traffic by implementing link-aware protection (LAP) system for wireless LANs. Our approach utilizes dynamic security policy management (DSPM) [9] to adapt to various protection policies depending on link quality. We have set up a real-time test-bed to evaluate our approach for VoIP traffic. Our contribution is many folds. First we show that how the performance of VoIP traffic is impacted by protection services in wireless LANs. Then, we present our dynamic solution, and discuss its implementation aspects in real-time scenarios. By presenting real-time results, we show that it is possible to achieve the required performance of VoIP under adequate protection in wireless LANs.

The rest of the paper is organized as follows. Section II

1-4244-1513-06/07/$25.00 ©2007 IEEE

shows the impact of protection services on VoIP performance through an experimental study. Various existing approaches to improve VoIP performance are discussed in Section III. Our proposed real-time system LAP, its associated modules, and its implementation details are explained in Section IV. In Section V, we first discuss specific modifications applied to LAP for VoIP traffic, explain switching criteria among different protection policies, and then demonstrate the VoIP performance with LAP in real-time scenarios. Finally, Section VI concludes the paper with brief discussion on future work.

II. Problem Decomposition and Motivation

Wireless LANs are becoming ubiquitous, and a broad range of applications, such as VoIP, video, and streaming audio/video, etc., are being used over them. As VoIP is becoming very popular in computer communication applications, we use it in this paper as a representative real-time application that is sensitive to packet losses and delay. We summarize the quality of service (QoS) in term of packet loss and delay required for VoIP [27].

- Packet Loss: It is recommended that packet loss should be less than 2% to experience good VoIP quality [27].
- E2E Delay: On the other hand, the end-to-end (E2E) delay should be less that 150ms for a good quality VoIP call [27].

By our real-time experiments, we demonstrate that such requirements may be difficult to achieve in wireless LANs with static configuration of protection services.

A. VoIP Traffic Emulation

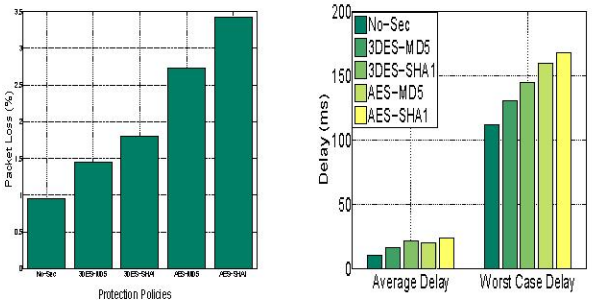
VoIP call is transmitted over Real-time Transport Protocol (RTP), which takes an audio codec's output, creates RTP packet (RTP header + voice payload) and passes it to UDP. We assume use of G.729 as audio codec which generates 10 bytes voice frames every 10 ms (i.e. at a rate of 8kbps) [6]. In real-life, some gateways aggregate two voice frames (2 x 10 bytes) to create one RTP packet (12 byte RTP header + 20 byte voice payload = 32 byte RTP packet) every 20 ms for improving efficiency [6]. Based on this, we emulate VoIP traffic in our real-time test-bed by transmitting UDP packets with 32 byte data at the rate of 50 packets/sec. We use *rude* utility to generate UDP traffic [5].

B. Protection Policies

To show the problem figuratively, we have collected experimental results in our real-time testbed with four protection policies. The four protection policies implemented in the testbed belong to IPSec security protocol suit, and are defined based on their uses of particular encryption and hashing algorithms. We use Openswan open source implementation [4] for IPSec which includes two options, advanced encryption standard (AES) and data encryption standard (3DES), for encryption algorithms, and two options, SHA1 and MD5, for hashing algorithms. Therefore, there are four ways, *AES-SHA1*, *AES-MD5*, *3DES-SHA1* and *3DES-MD5* to configure IPSec in our testbed. In this work, we refer these four possibilities as four IPSec protection policies. In general, AES and SHA1 are considered stronger mechanisms than 3DES and MD5, respectively. Moreover we observe in our previous study [8] that AES and SHA1 cause higher overhead than 3DES and MD5, respectively. The results show that, in general, stronger protection policies impose more performance overhead than weak protection policies.

C. Measurements Methodology

The measurements are taken in wireless LAN settings, where a client communicates with a policy server behind an access point by using four IPSec protection policies, discussed above. The policy server and access point are on the 3rd floor of a building, and the client is on the 2nd floor of the same building. This setting helps us in obtaining measurements with variations in the link connectivity between client and access points. The 2nd floor has a campus wireless network, however there is no wireless network on the 3rd floor except some students using their personal mobile devices. We observe that link variations are high during afternoon due to more students accessing wireless networks, whereas less link variations are observed during nights. We perform experiments during afternoon as well as nights to cover high and low link variations, respectively. With multiple round of experiments, we found a location where it is possible to achieve packet loss and worst case delay less than 2% and 100ms when no protection is applied. It means that VoIP's performance can be realized when there is no protection at the specified location. Although, we always perform experiments with some protection policy in our test-bed, case of no protection (*No-Sec*) is considered for comparison purposes. Further, every experiment during a particular protection policy has been carried out for 60 sec, in which UDP packets with payload size of 32 bytes are sent at the rate of 50 packets/sec. Total experiments associated with each protection policy are run for almost 2 hours. Experimental results for per packet delay (average and worst case) and packet losses are presented in Figure 1.



(a) Packet Loss. (b) Delay.

Fig. 1. VoIP performance under Different Protection Policies.

D. Observations

We observe from the Figure 1(a) that packet losses in case of no protection (No-Sec) are around 1% which is under the

limit for achieving VoIP performance. However, we notice that when protection services are applied, packet losses varies from 1.5% to around 3.5%. Therefore, we find that it is possible to use protection policies 3DES-MD5 and 3DES-SHA1 while maintaining required VoIP performance, but not AES-MD5 and AES-MD5, as they incur packet losses higher than 2%. In addition, we deduce from Figure 1(b) that average per packet E2E delay is well under 150 ms. This is due to the fact that VoIP traffic in our testbed is sent from a client to the policy server, which are separated by a wireless access point (one hop away). Therefore, average delay is not a concern in this setting. However worst case delay for policies 3DES-SHA1, AES-MD5 and AES-SHA1 is close to or longer than 150 ms, which may lead to packet losses due to dropping in playout buffer. Therefore, we deduce that it may not be possible to use protection policies 3DES-SHA1, AES-MD5 and AES-SHA1 in these scenarios.

An interesting point is that even though packet losses upto 3.5% does not seem very large, but due to stringent QoS requirements of VoIP, it is not possible to use stronger protection services while transmitting VoIP in wireless LANs. However, it is observed generally that a network does not require strong protection services always. It may be beneficial for a network to apply appropriate protection policy as required to achieve better performance. Therefore, in this paper, we propose a dynamic solution which ensures achieving required VoIP performance while maintaining sufficient protection most of the time. In this way, we are able to fulfill both performance and protection requirement for users using VoIP in wireless LANs. We will discuss our solution and its real-time implementation customized for VoIP traffic in a later section.

III. Related Work

As wireless networks are being considered to carry VoIP traffic efficiently, lots of research has been done to improve VoIP performance in the past, which can be categorized in following ways.

A. VoIP Performance Evaluations

Significant research has been devoted to understand the performance of VoIP in wireless networks. For example, authors in [12] demonstrate that only 6 voice calls can be supported with a specific voice codec in wireless LAN. They also show that the ongoing VoIP calls impact the effective available bandwidth for data traffic. In [10], authors evaluate the performance of VoIP in 802.11b DCF mode, and demonstrates that implementing a Backoff Control and Priority Queuing (BC-PQ) mechanism at the access points improves VoIP performance significantly. The reason is that BC-PQ provides higher priority to delay-sensitive packets such as VoIP packets, and allows them to use zero back-off value during contention. In addition, performance of VoIP under WEP and IPSec has been evaluated in [24]. These works either just demonstrate VoIP performance, or provide MAC layer solutions to improve VoIP performance. Our focus is different as we aim to provide an integrated solution where VoIP can coexist with protection service while maintaining required performance and protection.

B. VoIP Packet Aggregation Schemes

Small size of VoIP payloads with large size of headers from different network layers leads to inefficient transmission. Therefore, authors in [22] propose a packet aggregation scheme, called multiplex multicast (M-M), for downlink traffic from an access point to wireless clients. They suggest to multiplex more than one packets into one packet at the access point. The aggregated packet, then, is multicast to different wireless clients. Similarly, authors in [25] propose to aggregate packets at the access point for one call without creating delay, and demonstrate that their scheme can support more than 100 calls (using G.729 codec). Another scheme [23] to improve VoIP efficiency proposes to send a burst of packets after obtaining the medium after contention. Consequently, this scheme reduces the average waiting time and packet losses due to collision. In addition, the length of burst time is assigned a maximum value to control stations not acquiring the channel for very long time. These studies propose packet aggregation solution to improve VoIP performance without taking protection services into account. As our solution incorporates protection with VoIP, it can be used in conjunction with these packet aggregation schemes to improve performance further.

C. MAC Layer Solutions

Several MAC schemes are proposed for supporting VoIP in wireless LANs to reduce the delay for downlink VoIP traffic. For example, an Adaptive Priority Control (APC) is proposed in [19], in which AP is dynamically assigned a higher priority based on the uplink and downlink traffics. Another approach to improve VoIP performance dynamically adapts to the contention window based on the number of retransmissions in a system [14]. In addition, authors in [21] propose to use polling mode (PCF) instead of DCF in 802.11b, and show that increase in polling interval leads to support of more voice calls, however, with increased delay.

Existing studies either just show VoIP performance, or propose MAC layer solutions or require to aggregate packets to improve VoIP performance in wireless networks. Although our work can be used as an additional solution with the existing approaches to improve VoIP performance, our work is different from these studies in various aspects. First of all, we focus on VoIP in protected wireless networks (specifically wireless LANs), which means VoIP traffic has to co-exist with protection services. Second, our work involves monitoring of wireless link conditions, and the monitoring feedback is used to dynamically switch among protection policies to improve VoIP performance. Moreover, our work presents a real-time implementation of link-aware protection system (LAP) to show the feasibility that dynamic protection can be used in real scenarios to improve VoIP performance.

IV. Link-Aware Protection System (LAP)

In this section, we describe a real-time link-aware protection (LAP) system for improving VoIP performance in protected

wireless LANs. The basic assumption in LAP system is that it may be beneficial for a network to apply appropriate protection policies at different times as required to achieve better performance. Therefore, it is possible to switch between different protection policies based on some criteria. The criteria for switching among different protection policies used in LAP is based on the feedback about wireless link conditions. The wireless links conditions have been measured in terms of packet loss and E2E delay. Decision regarding switching among different protection policies is made after the wireless link performance has been measured. There are three modules associated with LAP to carry-out these operations. The schematic diagram of LAP system is presented in Figure 2, which includes three functional modules. The description of these modules is as follows.

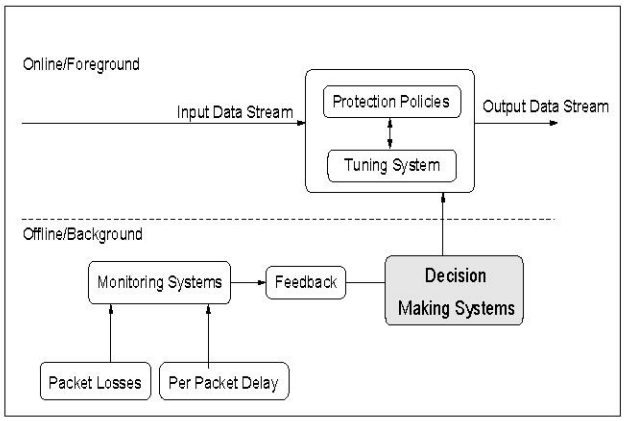


Fig. 2. Schematic Demonstration of LAP.

- **Monitor:** The monitor module collects statistics such as packet losses and delay over wireless links to measure a link performance. The monitor, then, provides the feedback to the decision-maker at regular intervals.
- **Decision-Maker:** Whenever the decision-maker module obtains feedback from the monitoring system, it runs an algorithm to determine the decisions regarding the switching of protection policies. The decision-maker, then, sends its decision to the tuner for switching. The monitor and decision-maker are executed as background processes so that they do not interfere with the ongoing data transmission in a system.
- **Tuner:** This takes care of changing the current policy to a new policy if the decision sent by the decision-maker includes new protection policy.

The theory and analysis associated with LAP is based on semi-Markov decision process (SMDP). Details of SMDP and its elements are presented in our previous work which proposes a generalized architecture called dynamic security policy management (DSPM) for wireless networks [9]. *This work is different from our previous work as follows.* We have proposed a modified scheme, called LAP, which is customized for loss and delay sensitive applications. For example, states in LAP system include one more element *delay* in addition to protection policy and packet loss. In addition, we discuss real-time implementation of LAP, and present experimental results unlike simulation results in our previous work. Moreover, we evaluate performance of LAP system, and demonstrate its usefulness for VoIP traffic in wireless LANs.

A. Real-Time Implementation

We have setup a wireless LAN testbed to implement dynamic protection system as shown in Figure 3. The testbed consists of a protection policy server behind an access point, and many mobile clients at different locations. The server is setup as a desktop machine, which provides negotiation of protection policies for clients in the wireless LANs. The clients are laptop computers and run an implementation of LAP system. The LAP system does not require any changes at the server side. The access point and clients use channel 6, and data rate has been set as 11 Mbps for all clients.

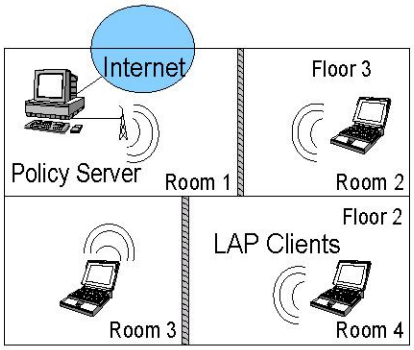


Fig. 3. LAP Testbed Setup.

1) Hardware Details: The server is Dell PC with Pentium IV (2.6 GHZ). We have used Cisco Access Points (Cisco Aironet 1200 series) to provide wireless connectivity. The mobile clients are Dell Laptop with Celeron Processor (2.4GHZ). In addition, we have used Lucent Orinoco gold wireless cards (802.11b) in mobile clients. All systems run Redhat Linux 9 with kernel version 2.4.20-8.

2) Software Details:

- **Openswan:** open source software is installed on the server and mobile clients for IPSec functionality [4].
- **OpenSSL:** open source software is installed on all systems to be used by IPSec protocol suite [2].
- **Rude** utility is used for emulating VoIP traffic [5].

3) IPSec Protection Policies: There are several security protocols such as Wired Equivalent Privacy (WEP) protocol, 802.1x framework with extensible authentication support (EAP) support, socket security layer (SSL), IP security (IPSec) and 802.11i designed to ensure protected communication over wireless networks [3], [7], [11], [15], [16]. WEP is supported in the firmware of wireless cards and the access point, and can be configured whenever required. However as WEP is not considered strong enough, its use is not recommended for wireless networks. Openswan [4] and Open1x [1] open source software of IPSec and 802.1x, respectively, are other

choices which can be used to configure different protection policy in the testbed. However, in this work, we use IPSec security protocol suite as a case study, as IPSec has been used widely to establish virtual private networks in wired and wireless networks, and is considered a strong security protocol.

As we use Openswan implementation of IPSec in this work, all details related to IPSec are specific to Openswan. In general, IPSec can be configured in tunnel and transport modes, however we use tunnel mode configuration as it is considered stronger than the transport mode. IPSec establishes tunnels between two end points, the server and the clients in our testbed, in two phases. In the first phase, called *Main Mode*, cryptographic keys to be used in the second phase are generated. In the second phase, called *Quick Mode*, encryption (AES, 3DES) and hashing algorithms (MD5, SHA1) are negotiated between the two end points and cryptographic keys are generated to be used for data transmission. In general, AES policies add 8 bytes more overhead to each packet than the 3DES policies. As VoIP packets are just 32 bytes (including RTP header), extra 8 bytes added by AES as compared to 3DES, leads to 25% extra overhead, and it can impact VoIP performance drastically.

Further, Openswan includes two modes of negotiation called *auto mode* and *manual mode* to establish tunnels. We use *auto mode* as it is more secure than *manual mode* due to automatic negotiation of cryptographic keys. In addition, we use public key cryptography for establishing tunnels between the server and clients, which is used during the first phase of IPSec negotiation. Moreover, to reduce the overhead associated with switching of protection policies, we configure four tunnels for four protection policies between the server and clients in advance. Therefore, switching of policies does not involve actual negotiation over wireless medium, instead it just requires to make the specific tunnel associated with the required policy active. Also, it ensures that no data packet is transmitted in clear, as any time there is always some tunnel active between the two end points. In addition, there are no packet losses involved due to switching among policies.

In addition, Openswan includes rekeying for providing better protection, and dead peer detection to check whether the other end is alive or not. We have disabled these features due to two reasons. First, we want to keep the overhead as low as possible due to negotiation. Since rekeying requires negotiation of the second phase and, therefore, leads to high packet delays during this negotiation. Second, as our real time experiments include scenarios with high packet losses sometimes, we notice several times that the negotiation for rekeying is not successful, and one end keeps trying for rekeying forever. Moreover, frequently one end interpreted that the other end is dead due to packet losses and tore down the tunnel, even though the other end is never dead.

4) Implementation of Monitor Module: The monitor module uses unicast probing technique to determine wireless link performance between a client and the server. Although, unicast probing technique creates more overhead than broadcast, but provides more accurate results due to the difference in transmission rates for broadcast data and unicast data. The monitor module calls traffic generator utility to send packets at a specified rate, and observes the responses. It estimates packet losses and average per packet delay, and then stores results in a file, called *mon-res*, to be read by decision maker. In this work, we measure the wireless link performance after every 3000 packets are sent at the rate of 50 packets/sec. The monitor module is written as awk script.

5) Implementation of Decision Maker and Tuner: As we discussed above, that we have pre-configured tunnels between the server and clients to reduce the switching overhead, so tuner module just needs to activate the appropriate tunnel based on results obtained from the decision maker module. Therefore, we have combined the functionality of both the modules in one module.

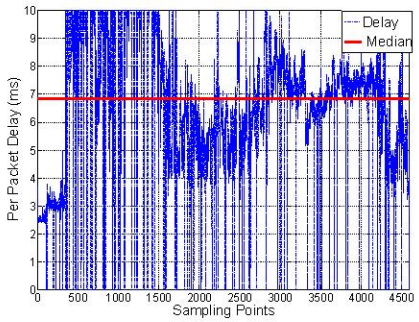
The decision maker module determines the appropriate protection policy to be used currently at the client based on the feedback obtained from the monitor module. To determine an appropriate policy, the decision maker calls *value iteration algorithm* as discussed in our previous work [9]. The value iteration algorithm outputs an action table which contains the protection policy to be used in each state of the system. As the action table is populated, the decision maker reads the file *mon-res*, and determines the appropriate policy for the system. If the current policy is the same as determined, then no switching takes places, otherwise the appropriate tunnel associated with the new security policy is made active. Both the modules are written as awk script as well.

V. Experimental Results

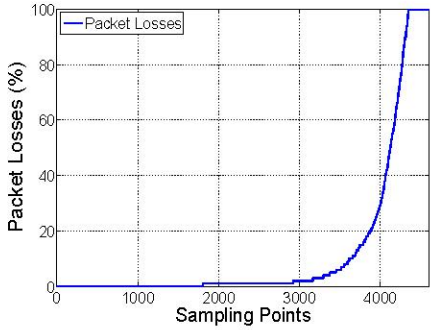
In this section, we present experimental results for VoIP traffic with real-time LAP system. We compare these results with the previous results in Section II, and demonstrate the usefulness of LAP for VoIP traffic in protected wireless LANs. Also, we give insights why LAP improves VoIP performance while maintaining adequate protection. We first present switching criteria used in LAP system customized for VoIP traffic.

A. LAP Switching Criteria

In this section, we discuss the criteria for switching among protection policies based on QoS requirements for VoIP. As VoIP's QoS demands less than 2% packet loss and 150 ms delay, we have taken these requirement into account for determining switching among policies. We performed real-time experiments by sending VoIP traffic in our testbed for approximately 20 hours. The packet rate used is 50 packets/sec and monitoring interval is 3000 packets (around 1 minute). We run these experiments without configuring any protection policy in the network so that VoIP performance can be measured without protection overhead. The results are presented in Figure 4, which shows the average delay and packet losses at different monitoring points. Then, the medians of packet loss and delay for these experiments are shown as the solid lines in the figure. We notice that medians for the average delay and packet loss are 7 ms and 1%, respectively. It is worthy of notice that the median for packet loss is 1% as desired by



(a) Delay Threshold.



(b) Packet Loss Threshold.

Fig. 4. Switching Criteria.

VoIP's QoS. It shows that the environment (or location where the client is placed) is good enough to have required VoIP performance. By doing this, we eliminate the problem due to *VoIP-unfriendly* environment with no way to achieve required VoIP performance. Now our focus is to deal with the overhead due to protection services which will be overcome by our LAP system. As the two end points for VoIP communication (the client and the server in our testbed) are just one-hop away, we reiterate the fact that average delay is not much concern in our testbed but the worst case delay. We term delay and packet loss medians as the packet loss ($P^\star$) and delay ($D^\star$) switching thresholds, respectively.

B. Protection Policy Switching Table

In this section, we present the switching sequence among policies based on the analysis presented in our previous work [9]. As channel conditions are characterized by packet loss (p_l) and delay (d) in LAP system, there are four possibilities depending upon (p_l) and delay (d) are less than or equal to $P^\star$ and $D^\star$, or greater than $P^\star$ and $D^\star$, respectively. Since, we use 4 IPSec policies for our measurements, our real-time LAP system can be characterized by using 16 states as four link conditions can be associated with each policy. State transition matrix in LAP assumes that it is possible to go to other states with the same probability. Now we obtain switching sequence by running value iteration algorithm as described in our previous work [9]. The final switching sequence obtained is shown in TABLE I. The real-time implementation of switching among policies is based on the TABLE I.

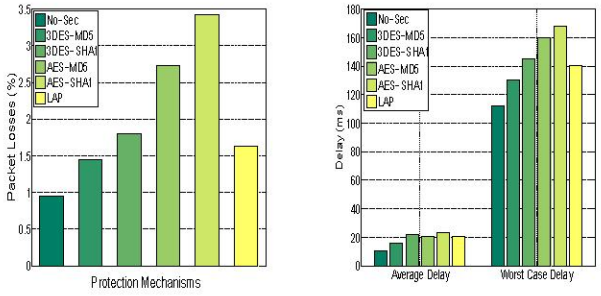
TABLE I

NEW PROTECTION POLICY IN EACH STATE.

Current Policy	New Policy			
	($p_l \leq P^\star$, $d \leq D^\star$)	($p_l \leq P^\star$, $d > D^\star$)	($p_l > P^\star$, $d \leq D^\star$)	($p_l > P^\star$, $d > D^\star$)
AES-SHA1	AES-SHA1	AES-MD5	3DES-SHA1	3DES-MD5
AES-MD5	AES-SHA1	3DES-SHA1	3DES-SHA1	3DES-MD5
3DES-SHA1	AES-SHA1	3DES-SHA1	3DES-SHA1	3DES-MD5
3DES-MD5	AES-SHA1	3DES-SHA1	3DES-SHA1	3DES-MD5

C. VoIP performance with LAP

We run around 100 experiments for each policy with each experiment with the rate of 50 packets/sec and monitoring interval of 3000 packets. Therefore, the total time for these experiments is approximately 1.5 hours. The experimental results and behavior of LAP system are presented in Figure 5 and Figure 6, respectively. Figure 5 is similar to Figure 1 except that the results for VoIP with LAP are also added in it.



(a) Packet Loss. (b) Delay.

Fig. 5. VoIP Performance with LAP.

We observe that packet losses with LAP are around 1.6% which is adequate for VoIP performance. Similarly, we notice that average delay and worst case delay are approximately 20ms and 140ms, respectively, which are also sufficient for achieving desired VoIP performance. The reasons for improved performance with VoIP can be explained based on TABLE II and Figure 6. We notice from TABLE II that the strongest protection AES-SHA1 is used for 62% of the total time, whereas policy 3DES-SHA1 is used for 33% of the time. An important conclusion is that to improve VoIP performance, LAP tuned itself based on the wireless link performance such that when a link experiences poor performance, LAP adapted to use a weaker policy like 3DES-SHA1. Therefore, the benefits of LAP are clear from the fact that while maintaining strong protection for 62% of the total time, LAP is able to offer desired VoIP performance.

TABLE II

POLICY DURATION.

Policy	AES-SHA1	AES-MD5	3DES-SHA1	3DES-MD5
Time(%)	62	2	33	3

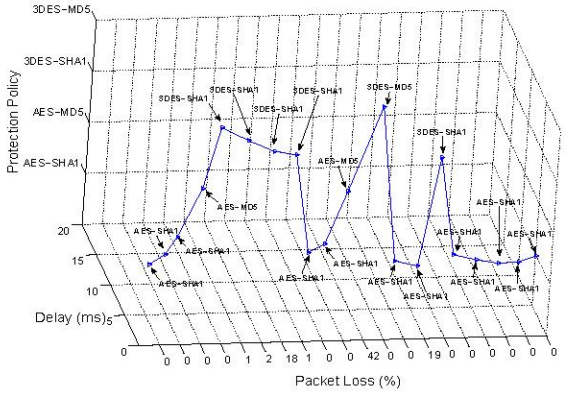


Fig. 6. A Snapshot of Switching Pattern.

To explain the LAP behavior further, we demonstrate how LAP switches among policies by presenting a snapshot of experiments in Figure 6. We notice that whenever packet losses are below its threshold but delay is higher than its threshold, LAP switches to 3DES-SHA1. Whereas whenever packet losses and delay both are below threshold, LAP switches to AES-SHA1. As policies AES-MD5 and 3DES-MD5 are utilized less, it means that most of the time client's link experienced low packet losses and sometimes higher delays due to retransmissions. Besides, the Figure 6 demonstrates how LAP adapts to link performance to improve VoIP performance in protected wireless LAN.

VI. CONCLUSION AND FUTURE WORK

In this paper, we addressed the issue of having real-time application such as VoIP together with protection in wireless LANs. To this end, we proposed a link-aware protection (LAP) system with dynamic switching among protection policies to achieve desired VoIP performance. We showed that the feedback about link performance in LAP is helpful in choosing adequate protection policy while maintaining the desired VoIP performance together in a system. We presented a real-time implementation of LAP system showing that performance of real-time applications such as VoIP can be improved by using dynamic protection. We believe that our work is an important and added advantage to the existing solutions real-time applications. To the best of our knowledge, this work is the first study which takes link conditions into account to dynamically tune various protection policies to improve application performance. In the future, we aim to implement LAP on a wireless network based robot navigation path tracking system, called Intelligent Space *(iSpace)*, which is a very useful platform for military applications [13].

REFERENCES

[1] 802.1x Supplicant. *http://www.open1x.org*.

[2] *OpenSSL*. *http://www.openssl.org*.

[3] IEEE 802 Standards. *http://standards.ieee.org/getieee802*.

[4] IPSEC. *http://www.openswan.org*.

[5] Rude. *http://rude.sourceforge.net/*.

[6] VoIP in Cisco Gateways. *http://www.cisco.com/warp/public/788/pkt-voice-general/bwidth_consume.html*.

[7] IEEE Std 802.1x-2001x: Port-Based Network Access Control. *http://www.ieee802.org/1/pages/802.1x.html*, June 2001.

[8] A. K. Agarwal and W. Wang. On the Impact of Quality of Protection in Wireless Local Area Networks with IP Mobility. *ACM Mobile Networks and Applications (ACM MONET)*, 12(1):93–110, February 2007.

[9] Avesh K. Agarwal and Wenye Wang. DSPM: Dynamic Security Policy Management for Optimizing Performance in Wireless Networks. In *Proc. of IEEE Milcom'06*, October 2006.

[10] F. Anjum, M. Elaoud, D. Famolari, A. Ghosh, R. Vaidyanathan, A. Dutta, P. Agrawal, T. Kodama, and Y. Katsube. Voice Performance in WLAN networks - An Experimental Study. In *IEEE GLOBECOM '03*, volume 6, pages 1–5, December 2003.

[11] N. Borisov, I. Goldberg, and D. Wagner. Intercepting Mobile Communications:The Insecurity of 802.11. In *Proc. of the ACM MobiCom'01*, pages 180–189, July 2001.

[12] S. Garg and M. Kappes. An Experimental Study of Throughput for UDP and VoIP Traffic in IEEE 802.11b Networks. In *IEEE WCNC, 2003*, volume 3, pages 1748–1753, March 2003.

[13] R. Gupta, A. K. Agarwal, W. Wang, and M.-Y. Chow. Characterization of Data-Sensitive Wireless Distributed Networked-Control-Systems. In *Proc. of the 2007 IEEE/ASME International Conference on Advanced Intelligent Mechatronics*, September 2007.

[14] G. Hanley, S. Murphy, and L. Murphy. Adapting WLAN MAC Parameters to Enhance VoIP Call Capacity. In *Proc. of the 8th ACM MSWiM'05*, pages 250 – 254, October 2005.

[15] A. Hecker and A. H. Laboid. A New EAP-Based Signal Protocol for IEEE 802.11 Wireless LANs. In *Proc. of the IEEE 60th VTC Fall'04*, volume 5, pages 3214–3218, September 2004.

[16] A. Hecker and A. H. Laboid. Pre-Authenticated Signaling in Wireless LANs using 802.1X Access Control. In *Proc. of the IEEE Global Telecommunications Conference (GLOBECOM'04)*, volume 4, pages 2180–2184, November-December 2004.

[17] T. Karygiannis and L. Owens. Wireless Network Security 802.11, Bluetooth and Handheld Devices. *National Institute of Technology, Special Publication*, pages 800–848, November 2002.

[18] Kelvin K. Lee and Samuel T. Chanson. Packet Loss Probability for Real-Time Wireless Communications. *IEEE Transactions On Vehicular Technology*, 51(6):1569–1575, Novembe 2002.

[19] H. Schulzrinne S. Shin. Balancing Uplink and Downlink Delay of VoIP Traffic in WLANs Using Adaptive Priority Control (APC). In *Proc. of the 3rd International Conference on Quality of Service in Heterogeneous Wired/Wireless Networks, QShine'06*, August 2006.

[20] S. Tsao. Research Challenges and Perspectives of Voice over Wireless LAN. In *IEEE EITC, 2005*, August 2005.

[21] M. Veeraraghavan, N. Cocker, and T. Moors. Support of Voice Services in IEEE 802.11 Wireless LANs. In *IEEE INFCOM, 2001*, volume 1, pages 488 – 497, April 2001.

[22] W. Wang, S. C. Liew, and V. O. K. Li. Solutions to Performance Problems in VoIP Over a 802.11 Wireless LAN. *IEEE Transactions on Vehicular Technology*, 54(1):366 – 384, Januray 2005.

[23] X. G. Wang, G. Min, and J. E. Mellor. Improving VOIP Application's Performance over WLAN Using a New Distributed Fair MAC Scheme. In *IEEE AINA, 2004*, volume 1, pages 126 – 131, 2004.

[24] H. Xiao and P. Zarrella. Quality Effects of Wireless VoIP Using Security Solutions. In *IEEE MILCOM, 2004*, volume 3, pages 1352 – 1357, November 2004.

[25] S. Yun, H. Kim, and I. Kang;. Squeezing 100+ VoIP Calls Out of 802.11b WLANs. In *IEEE WOWMOM, 2006*, June 2006.

[26] Y. Zahur and T. A. Yang. Wireless LAN Security and Laboratory Designs. *Journal of Computing Sciences in Colleges*, 19(3):44–60, January 2004.

[27] H. Zhai, X. Chen, and Y. Fang. How Well Can The IEEE 802.11 Wireless LAN Support Quality of Service? *IEEE Transactions on Wireless Communications*, 4(6):3084–3094, November 2005.