Telematics and Informatics 27 (2010) 377–393

Contents lists available at ScienceDirect

Telematics and Informatics

journal homepage: www.elsevier.com/locate/tele

A remote interactive non-repudiation multimedia-based m-learning system

Sasan Adibi *

ECE Dept., University of Waterloo, Waterloo, ON, Canada N2L 3G1

ARTICLE INFO

Article history:
Received 8 June 2009
Received in revised form 27 November 2009
Accepted 12 January 2010

Keywords:
m-Leaning
e-Learning
Non-repudiation
Identity management
Multimedia interactive communication

ABSTRACT

One of the current challenges regarding distance learning systems, from a performance point of view, is the efficient and timely delivery of multimedia-enriched learning materials. Providing guaranteed Class of Service (CoS) and Quality of Service (QoS) are also challenging especially for remote sites and rural areas where Internet coverage tends to be limited. On a different note, another challenge is to track the audience accessing the learning materials and more importantly to monitor the true identity of the examination attendees. This paper aims to investigate both of these issues simultaneously, with an introduction of a non-repudiation system that provides a security mechanism, as well as maintaining certain QoS measures. This system not only authenticates the intended party, but also integrates a digital signature scheme accompanied with the transmitted multimedia-based information. The included digital signature prevents a later dispute from the involved parties that the communication ever took place or they ever took part in the communication.

Therefore this paper introduces and discusses a multimedia-enriched interactive non-repudiation system involved in a mobile-based learning (m-learning) environment. The performance of this system is considered and discussed in terms of network-centric parameters, including end-to-end delays, overhead, and bandwidth, using Labview 8.5 mobile-transmitter and mobile-receiver testbeds.

1. Introduction

In this paper we study the security requirements of m-learning systems and develop an application layer non-repudiation multi-level signature-based system, which features a biometric scheme to create digital IDs. These IDs are based on both unique device and biometric characteristics, specific to each user, which we refer to as: *identity data* or *digital ID*. Digital signatures will be created based on a digital ID. In parallel, three cross-layer-based parameters are extracted and imported to the application layer and the application layer encoder takes these parameters into account for proper multimedia encoding. A hash function is then applied to the entire data payload (identity data, cross-layer information, and the generated digital signature), and the resulted hash value is added to the pre-hashed payload and the entire information is packed in the UDP (User Datagram Protocol) payload. The hash value is used to prevent any unnoticed illegitimate changes to the UDP payload. The UDP packet streams are then further processed at lower layers (i.e., network, MAC, and physical layers) and transmitted via a Wi-Fi link. The sender and the receiver can both be on the same Distributed System (DS), in which case the entire end-to-end path will be explicitly wirelessly. The sender and receiver can also be located in two different geographical locations, in which case, the end-to-end data path may include several hops with partial wired segments.

* Tel.: +1 519 888 4567.
E-mail address: sadibi@uwaterloo.ca

0736-5853/$ - see front matter © 2010 Elsevier Ltd. All rights reserved.
doi:10.1016/j.tele.2010.01.001

Once the UDP payloads are received and unpacked, the three components: identity data, cross-layer information, and the digital signature are separated and used accordingly. The digital signature and the subsequent identity data are used to correctly identify the user proper user/device identification and for a non-repudiation purpose. The performance of this system is discussed in details using analytical and real data transmission flows simulated by Labview 8.5.

The organization of this paper is as follows: Section 2 discusses the current security approaches in m-learning scenarios. Section 3 is focused on the system's overall architecture and algorithm. Section 4 discusses application layer, including the cross-layer interaction and the multimedia encoding. Section 5 considers the required handling at the transport, network, MAC, and PHY layers. Section 6 presents the details of the multi-layer system design. Section 7 includes the Quality of Service (QoS) performance discussions, including; end-to-end delays, jitter, and bandwidth figures. Section 8 presents the security analysis of the system. Section 9 provides the conclusion following by the reference.

2. Current Implementations

Electronic-learning (e-learning) is a learning method where the involved parties are usually in different geographical locations and the instruction information are passed through computer networks and viewed by computer-based systems. e-Learning systems and techniques have evolved over the recent years and have progressed to a limit that face-to-face interactions are becoming less required. In particular, various conferencing technologies, including; teleconferencing (voice-based), videoconferencing (video based), and web-conferencing (e.g., webinars, webcasts), are mostly based on prerecorded teaching episodes or entirely animated scenes, requiring no real person to conduct live lectures and presentations. In most cases, both video streaming (for video contents) and Voice over IP (VoIP, for voice contents) protocols are merged to convey the entire lecture/presentation data delivery. Text-chats and email services are often used to send feedbacks, responses to comments, and asking questions from the instructors. The voice/video/text/email facilities require real-time with limited round-trip delays and sufficient guaranteed bandwidth for optimum performance. For voice and video, there is a major emphasis on the real-time protocol supports requiring bounded delays and jitter (variable delays) figures with minimum guarantee of bandwidths. Text-chat and email services are often less bounded to these limitations and a non-real-time protocol is actually sufficient to convey these messages. Therefore a relatively large amount of delays (a few seconds to a few tens of seconds) would be acceptable for text and email messages.

2.1. Content sharing

Content sharing and videoconferencing are two concepts with similar approaches. The basic idea encompasses two sets of video streams enabling both parties to view the participants at remote locations for graphical and material presentation purposes.

H.239 is an ITU-T recommendation based on the H.3xx class of multimedia communications standard group (i.e., H.323) that offers additional media channels for H.3xx terminals and role management (H.239, 2009). H.239 features a dual-video streaming function using Session Initiation Protocol (SIP) Hautakorpi and Camarillo, 2007. The streaming parameters for SIP are described with the Session Description Protocol (SDP) based on RFC (Request for Comment) 4796 and RFC 4574 (Hautakorpi and Camarillo, 2007; Levin and Camarillo, 2006), where the content "label" attribute is defined (Hautakorpi and Camarillo, 2007; Levin and Camarillo, 2006; Karapetkov, 2008). Other RFCs that discuss the media control in terms of content sharing, include (Camarillo et al., 2002; Camarillo et al., 2006; Camarillo, 2006); Grouping of Media Lines in SDP (RFC 3388), Binary Flow Control Protocol (BFCP) RFC 4582), and SDP Format for BFCP Streams (RFC 4583).

2.2. e-Learning versus m-learning

e-Learning technologies were introduced back in 1993 when limited computer/email-based interactions were available (Electronic Learning, 2009). e-Learning, flexible learning, and distance learning definitions often go hand-in-hand and the goal of such learning methods is to provide maximum location independency and flexibility to receive learning materials via online and media-based (e.g., CD and DVD) technologies.

The emerging web technologies have had profound effects on the quality of e-learning methods. Web 1.0 is a term referring to the early concepts of content delivery using basic web design technologies, including; HTTP (Hypertext Transfer Protocol) and HTML (Hyper Text Markup Language). Web 2.0 is the most recent term referring to the next generation of web-related applications and content delivery and presentations that facilitates secured multimedia-enabled information sharing. Web 2.0 includes the following concepts: Social Work 2.0, online interactions (e.g., blogs), XML (Extensible Markup Language), RSS (Really Simple Syndication) feeds, social networking protocols (e.g., FOAF "Friend of a Friend" and XFN "XHTML Friends Network"), and Web APIs (Application Programming Interfaces, such as; REST "Representational State Transfer" and SOAP "Simple Object Access Protocol") (Web 2.0, 2009).

m-Learning (mobile-learning) is also on the same track as e-learning, however features distinct device/application utilization, which is based on mobile or other types of portable devices in the e-learning process. M-learning is completely location independent, which means that the m-learning session can take place virtually in any location (e.g., taxi, restaurant, street, etc.).

As cell-phone data-plans continue to decrease in price and increase in versatility and include more affordable contract terms (i.e., unlimited data usage), more people are considering m-learning more attractive than e-learning, due to the fact that e-learning scenarios require the learners to be in a fixed location or with a limited mobility throughout the data learning delivery, mostly through the Internet.

There are however a few challenges associated with m-learning, including: limited battery life on mobile devices, variable wireless coverage and having limited or no coverage in some rural areas, and limited key and screen sizes (MLearning, 2009). Current Smartphone platforms, such as in Blackberry Storm and Apple iPhone, have remedied the screen and key sizes to some extent and the new technologies in the wireless domain fronts, including usage of localized cell coverage (i.e., femtocell Markendahl et al., 2008) and directing cellular traffic through the Wi-Fi Access Point (AP) using UMA (Unlicensed Mobile Access) technology (Arjona and Verkasalo, 2007), have also eased the wireless coverage issues slightly. The battery life issue is still the major challenge, though several power-save operation modes have been introduced and implemented in various cellular and Wi-Fi protocols, including: UAPSD (Unscheduled Automatic Power Save Delivery) in IEEE 802.11e (Pérez-Costa et al., 2006) and SMPS (Spatial Multiplexing Power Save) and PSMP (Power Save Multi Poll) in IEEE 802.11n (Nesimoglu et al., 2008).

2.3. Security requirements for m-learning systems

Security for both e-learning and m-learning systems is of great importance. In an end-to-end sense, there are various security concerns that need to be addressed, which are summarized in Table 1.

Table 1 shows various security threats, cause of lack of security, and security remedies for m-learning systems, which can be categorized in the following action items:

(1) *Client/server/service/instructor identifications* require strong authentication schemes to ensure legitimate entities have access to the associated channel(s). The strongest form of client/server authentication is a mutual authentication, also known as; a two-way authentication scheme, which requires both client and server to be authenticated to one another using a symmetric authentication method (List of Identity Management Terminology, 2009).
(2) *Message privacy* is required for each channel to convey secure communicates between server/instructor/users, which can be achieved by a strong encryption technique.
(3) *Message integrity* is a security mechanism in which the privacy of messages is not an issue, however the messages should not be altered by any illegitimate entity. This can be achieved by using a message digest or hashing function.
(4) *Non-repudiation* schemes prevent legitimate users, which have already taken part in a communication to deny their involvements.
(5) *Man-in-the-Middle (MitM)* attack is a security breach in which an illegitimate entity masquerades as a legitimate user or a server and steals the credentials of a legitimate user or server, which may start a new session using the stolen credentials to gain access to the channel for further attacks.
(6) *Denial of Service (DoS)* attacks are complicated sets of multilayer attacks in which the intruder jams the related channel/layer with exhaustive queries to prevent legitimate users from gaining access to the channel, accelerating the power consumption, draining the scarce battery power.

In this paper, we will be focusing on the non-repudiation security issue, which is an important mechanism in an m-learning environment, especially for correctly monitor who participates in the learning sessions (for billing purposes) and who is really taking the tests in the examinations. The following references are concerning non-repudiation mechanisms.

Stach and Park (1998) propose a simple non-repudiation protocol that establishes a trust link between the Mobile Unit (MU) and Visiting Location Register (VLR) in a GSM (Global Systems for Mobile communication) Personal Communication System (PCS). The non-repudiation protocol adds overhead to a call, especially in the origination and termination periods. The performance of this system is studied in terms of velocity of the handset mobility starting from 5.6 km/h gradually increasing up to 89.6 km/h for different origination rates. It shows that the added overhead (up to 23%) has negligible effects on the quality of the conversation.

Table 1
m-Learning security issues, observations, and remedies.

Security issue	Cause of lack of security	Security remedy
Client security	Illegitimate user accessing one channel	Strong client authentication
Server security	Illegitimate entity servicing over many channels	Strong server authentication
Service security	Illegitimate service running on many channels	Strong service ID authentication
Instructor security	Illegitimate admin accessing all channels	Strong admin authentication
Message privacy	Messages contents exposed to illegitimate users	Strong encryption algorithm
Message integrity	Messages altered by illegitimate users	Strong hashing algorithm
Non-repudiation	Legitimate users deny their involvements in a session	Strong digital signature algorithm
MitM Attack	Illegitimate user masquerading a user or a server taking over a session	Strong symmetric mutual authentication scheme
DoS Attack	Service unavailable to legitimate users	Multilayer deterrence schemes

Kritzinger and von Solms (2006) discuss the e-learning/m-learning (e/m-learning) systems security requirements and propose four main security pillars:

Pillar 1: e/m-learning information security governance support
Pillar 2: e/m-learning information security procedures and policies
Pillar 3: e/m-learning information security countermeasures implementation
Pillar 4: e/m-learning information security countermeasures monitoring.

Pillar 3 contains six main security requirements, including: *Identification*, *authentication*, *authorization*, *confidentiality*, *integrity*, *non-repudiation*, and *availability*. It should be noted that availability is a probabilistic measure of how available the resources are?

Bechelli et al. (2002) incorporate biometric technologies for remote authentication applications. For instance; finger print, iris, face, and voice authentication methods are currently being used to authenticate remote access. In this reference, biometric methods are used for not only authentication, but also for creating digital signatures (based on X.509 certificate schemes) to be used for non-repudiation purposes. This can directly be used in an m-learning system. Biometric schemes will be discussed in more detail in Section 2.4.

Hinard et al. (2006) propose a multicast streaming application with security and Quality of Service (QoS) supports. The security option provides data origin authenticity and the QoS option offers received stream quality adaptation technique. The data origin authenticity involves digital signature propagation, offering continuous non-repudiation and integrity schemes in a layered manner for media streaming video scenarios. The performance of the proposed schemes is evaluated using NS-II (Network Simulator) software against various network conditions. The performance shows efficient results against bursty and lossy network conditions.

Anwar and Greer (2006) suggest a context-based identity and guarantor-mediated reputation management system that involves a repudiation transfer model without compromising identity, therefore providing trust while preserving anonymity. The repudiation transfer model involves several functional entities, including: Actor, key generator, guarantor, and repudiator. An actor is a participant in an m-learning scenario (e.g., student or instructor). The repudiator is an agent that assesses the trustworthiness of the actor. The guarantor is a trusted public witness agent that oversees all activities, which is directly involved in the non-repudiation scheme. The key generator is a trusted key generation entity that provides Public Key Infrastructure (PKI).

Weippl and Ebner (2008) discuss security challenges in e/m-learning 2.0 systems. As mentioned before, Web 2.0 is the new generation of web technologies that facilitates online interactions, offering enhanced multimedia capabilities. However increased capabilities are often coupled with more advanced risks and threats. The e/m-learning 2.0 security risks include weak web applications and plagiarism. Since we are dealing with client/server scenarios, most of the client/server security issues apply to e/m-learning scenarios. As for plagiarism, anti-plagiarism software and non-repudiation schemes are being used to reduce this risk.

Raitman et al. (2005) address the collaborative e/m-learning environment security roles, mostly discussing the importance of social identity aspects, including online collaborations and wiki platforms. This reference argues that the main social security pillars are based on *confidentiality*, *integrity*, and *availability*. It also emphasizes the importance of secured logging systems with three security abilities: *auditing*, *accountability* and *non-repudiation* capabilities. The proposed scheme records all students/instructor actions with a built-in traceability feature.

Yong (2007) provides a general discussion covering security attributes relevant to all e/m-learning participants, regulator, stakeholder and administrative staffs. These attributes include: *Compulsory Attribute* (*CA*), *Optional Attribute* (*OA*), *Obvious*

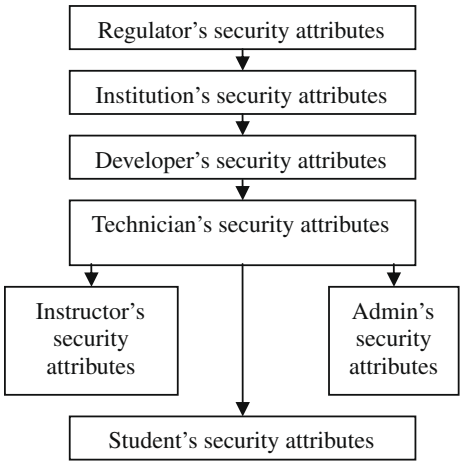

Fig. 1. e/m-Learning security model.

Attribute (*ObA*), and *Hidden Attribute* (*HA*). The non-repudiation mechanism is required for the CA, not applicable to OA, acceptable to ObA and unacceptable to HA.

The results of this discussion are considered in the creation of the e/m-learning security model, which is shown in Fig. 1 (adapted from Yong (2007)).

In general, all e/m-learning systems require proper security consideration and implementation to be in place. Non-repudiation techniques play a major role in distance learning systems, which may feature not only a traditional username/password scheme to be in place, however biometric measures with controlled network-related parameters (e.g., authentication latency) may be needed (Nickolova and Nickolov, 2007; Park et al., 2007; Diab et al., 2008).

2.4. Identity management in m-learning schemes

The identity management is a broad terminology that deals with identifying individuals in closed or open systems and controlling how they access the resources according to restrictions linked to each individual. In an m-learning scenario, username–password alone may no longer be sufficiently accepted as a strong identity verification measure, therefore other means are required for a strong identity management scheme, including biometric, device-level, and multi-level authentication and encryption schemes.

2.4.1. Biometric security measures

Biometric authentication and encryption schemes are used to transform user initiated biometric data into untraceable biometric information. There are various biometric measures used for authentication and encryption/decryption mechanisms, including: face, fingerprints, iris colors and patterns, hand/finger geometries, voice, dynamic signature, keystroke dynamics, gait, and DNA schemes. The information contained in biometric measures is unique and irrevocable.

Biometric Authentication (BA) and Biometric Encryption (BE) mechanisms bind physical characteristics of a biometric feature (e.g., voice, fingerprint) into digital keys, called; biometric template. The biometric template digital information is bound to randomly generated keys through BE binding algorithm to form biometrically encrypted keys, which are used to encrypt messages. To decrypt the messages, the same biometric feature is required to be present and the reversed algorithm will produce the plaintext. Neither the keys, nor the biometric physical characters can be retrieved from the stored BA/BE template. A biometric dependent helper data is always stored in the system to assist the encryption/decryption fuzzy processes. The fuzziness of the processes is due to the natural variability of biometric measures (Stoianov, 2008).

There are two parameters, which impact the biometric performance, which are; False Rejection Rate (FRR) and False Acceptance Rate (FAR). The FRR defines the percentage of false rejections and the FAR gives the percentage of false acceptance.

Among all biometric features, the most promising results have been achieved through iris-based encryption techniques (Cavoukian and Stoianov, 2007). Iris's FRR is 0.47% and FAR is 0% (less than 0.0005%) and can be used to produce a key of up to 140 bits. The second best accuracy is achieved by fingerprint with an FRR value of less than 10%. Fingerprints are more prone to distortion and inaccuracy. The third best biometric feature is achieved through face recognition, with a variable FRR values from 3.5% to 35% and an FAR value of less than 0.001%. Face-based encryption key can be up to 58 bits, which when used alone may not be enough in many security scenarios. Voice-based signatures may not have enough entropy (non-redundant information) to create strong encryption keys, therefore another security scheme needs to be accompanied with voice to result in a strong identity management scheme, such as a user-based password.

2.4.2. Device authentication

Each device used as an end-point has a unique ID (e.g., MAC address), which can be used in the authentication scheme. A relatively weak biometric authentication technique, such as voice, can be accompanied with the device-level authentication scheme to produce a rather strong authentication mechanism. The device ID can not only be used for authentication purpose, but it can also be used in the digital signature creation scheme (e.g., using X.509). Another similar authentication scheme makes use of the location (e.g., location-based scheme), which can be linked to the device properties.

2.4.3. Multilayer authentication schemes

A very strong authentication technique may feature a multi-layer approach, where each authentication scheme feeds a specific protocol used between two end-points. For instance, the iris-based authentication scheme may be used at the application layer where user-based interactions are formed and messages and dealt with. At the same time, a fingerprint authentication scheme may be linked to the device authentication and be used at the transport layer (e.g., TCP and UDP) or network layer (e.g., IP). This way a multi-level biometric authentication scheme is created, which features multiprotocol-level (as well as multiservice-level) and device-level authentication mechanisms.

3. System's architecture

Fig. 2 shows the proposed system's flowchart, which includes a digital signature processing unit that is fed by the biometric authentication unit and outputs digital signature information. This system is able to transmit multimedia traffic (text, voice, and video), digital signature, and cross-layer data simultaneously. The cross-layer data, as mentioned, is used to

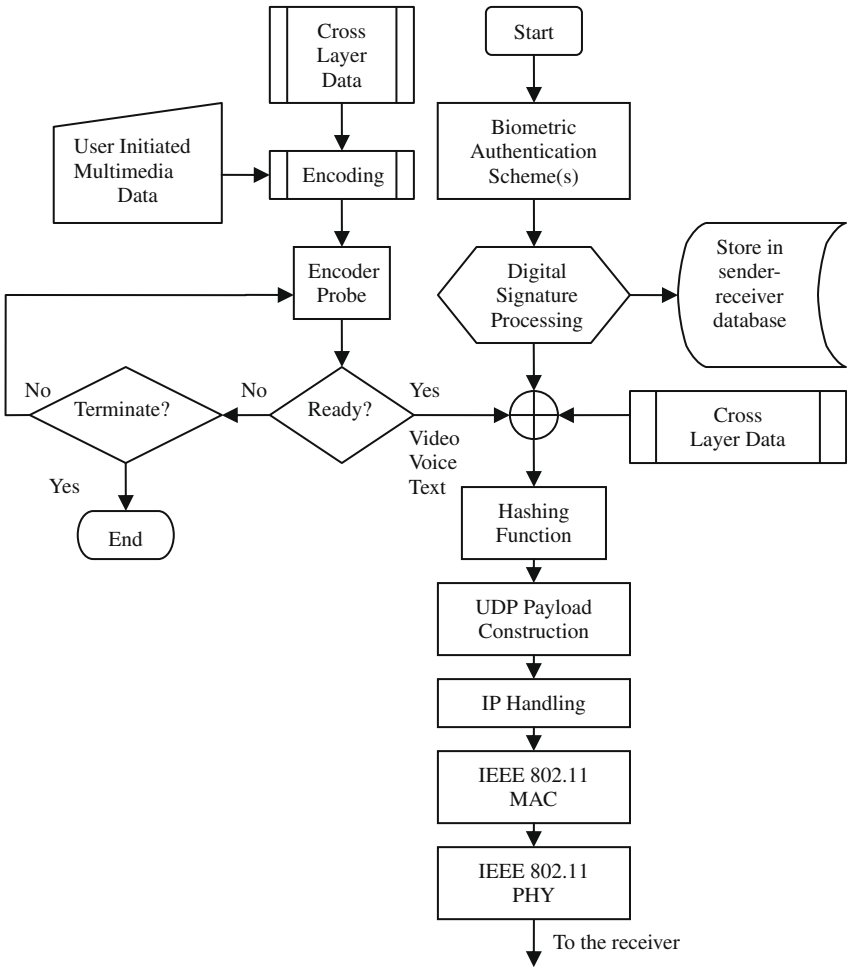

Fig. 2. Non-repudiation multimedia-based system architecture.

optimize the multimedia encoding function. For voice; G.711 and for video; H.264 codecs are used. These codecs are explained in a later section. Once these three data pieces are available, a hashing function is then applied (in addition to the hash function applied by the digital signature), which creates a message digest. A message digest is a fixed-size message with specific attributes, which will be discussed in a later section. All these processes take place at the application layer.

These four individual data pieces are then moved to the transport layer and packed in the UDP's payload. The packets are then moved down to network, MAC and PHY layers and appropriate functions are applied before transmitted onto the medium. Network layer provides IP data handling, including DSCP (DiffServe Code Point) QoS setting and IPSec (IP Security) functionality. In terms of QoS and security, the MAC layer offers services provided in the IEEE 802.11e (IEEE 802.11e-2005, 2009) and IEEE 802.11i (IEEE 802.11i-2004, 2009) standards. IEEE 802.11e provides EDCA (Enhanced Distributed Channel Access), which assigns different traffic priorities to different traffic queues, therefore queues with high priority labels can potentially transmit first. IEEE 802.11i is an IEEE 802.11 amendment for security purposes. It provides security extensions on top of WEP (Wired Equivalent Privacy) (Wired Equivalent Privacy, 2009), including WPA (Wi-Fi Protected Access) (Wi-Fi Protected Access, 2009).

The proposed system can be used efficiently in a Wi-Fi enabled m-learning scenario. A similar discussion can also be applied to cellular-based m-learning scenario.

The proposed system can be used both for local and remote scenarios. Both student and instructor (sender and receiver) can be located on the same DS being served by the same Access Point (AP), as well as in two different continents across multiple Wide Area Networks (WANs). The network layer; IP, handles routing-related issues, as well as secure routing, using Virtual Private Networks (based on IPSec).

4. Application layer functions

At the application layer, we are dealing with messages and security processes can be applied to messages rather than packet-level processing. Here are the functions taking place at the application layer:

4.1. Digital signature scheme (based on digital ID)

The process start from a biometric authentication scheme, which can be based on one of the following schemes: iris, fingerprint, face, or voice. There are three outcomes from the biometric authentication scheme: (1) correctly authenticating and registering valid users, (2) creating encryption/decryption keys, and (3) generating digital signatures for the purpose of non-repudiation mechanisms. The biometric system should be able to produce a key system with more than 128-bit hey information for an acceptable encryption/decryption mechanism, which can be used in the encryption system, as well as for the digital signature scheme. If the biometric scheme is not able to produce enough key bits, other security means (e.g., user-based password) should be accompanied with the biometric system.

A digital signature is the mechanism that provides message integrity and non-repudiation. Therefore the recipient is able to correctly identify the real originator of the transmission and to ensure the message has not been altered without the originator's knowledge. In some schemes, encryption would also be required to ensure that the information has not been revealed to outsiders, thus providing privacy.

A digital signature usually consists of three steps: (1) key generation (public/private key pair), (2) signing operation, and (3) verification.

There are several well-known digital signature schemes, namely; DSA (Digital Signature Algorithm, 2009) and RSA (Ron Rivest, Adi Shamir, and Leonard Adleman) (RSA, 2009), which will both be considered in this system design.

4.2. Multimedia encoding

The codecs (G.711 and H.264) used for voice and video conversations operate efficiently in Wi-Fi-based systems. In a cellular-based mobile system, these codecs may require a 3G; third Generation mobile network access, such as: USDPA (High-Speed Downlink Packet Access) and HSUPA (High-Speed Uplink Packet Access) systems for the most efficient multimedia usage, otherwise less bandwidth demanding codecs should be used. Table 2 (Voice Over IP – Per Call Bandwidth Consumption, Cisco Systems, Document ID: 7934, 2006; Bandwidth Calculator for VOIP, 2006; VoIP Bandwidth Calculation, Newport Networks, 2005; Zhao et al., 2003) shows different codec types, which vary in terms of coding techniques and data rates (quality). The G.711 codec requires a relatively high data rate, which might not be suitable for 2G; second Generation mobile networks, such as GSM (Global System for Mobile Communications) based devices, in which case, a lower data rate codec may be more suitable, such as G.723.1 that can operate as low as 5.3 kbps instead of 64 kbps.

Table 3 (Video Conferencing Standards, 2009; Wiegand, 2007; Topiwala and Jindal, 2004) displays H.263, H.264, and MPEG-4 video codecs and their technical specifications. H.264 runs also at 64 kbps and higher, which provides a relatively good video quality for handheld Wi-Fi-enabled devices. For cellular-based systems operating on 2G networks (i.e., GSM), video codecs with lower data rates (e.g., H.263) can be used. More detailed analysis on the multimedia will be given in a later section.

4.3. Hash function

A Hash or a Message Digest (MD) is a mathematical function that takes a random number of bits (limited by the minimum and maximum number of data bits) as inputs and creates a fixed-length output string with the following general specifications:

(1) Disregarding the number of input bits, the output string is fixed length
(2) A single bit difference between two input data should result in a close to 50% change in the hash's output strings
(3) Very low probability that the hash of two different input data produces the same output string (collision).

Table 2
Different audio codecs and their specifications.

Audio Codec	Coding technique	Data rate (kbps)
G.711 (A-, μ-law)	PCM	64
G.722	ADPCM	48, 56, 64
G.722.1	ACELP	24, 32
G.722.2	ACELP	23.85
G.723.1	ACELP/MPC-MLQ	5.3, 6.4
G.726	ADPCM	24, 32
G.728	LD-CELP	16
G.729	CS-ACELP	6. 4, 8, 11.8
G.729a	CS-CELP	8
AMR-WB (G.722.2)	ACELP	6.6–23.85
AMR-WB+	ACELP	5.2–48

Table 3
Different video codecs and their specifications.

Video Codec	Algorithm	Format specific properties	Data rate (kbps)
H.263	OBMC, DCT, SQCIF, QCIF, CIF, 4CIF, 16CIF	128 × 96, 176 × 144, 352 × 288, 704 × 576, 1408 × 1152 – up to 72 fps	10–64 (audio) 1024–20,480
H.264	4 × 4 DCT, 8 × 8 DCT	Similar to MPEG-4	64–983,040
MPEG-4		Level 4, 720 × 1280 progressive, 1080 × 1920 interlace	24–24,5760

A message digest, if transmitted along with the original message, will provide message integrity. Therefore if the message is altered illegitimately, the receiver calculates the hash value based on the received message and since the original message has been changed, the hash values will be different, which informs the receiver about the illegitimate message alteration.

A few Secure Hash Algorithm (SHA) schemes include: SHA-0, SHA-1, SHA-256, SHA-384, and SHA-512 (SHA hash functions, 2009).

4.4. Cross-layer function

The cross-layer design involves interlayer exporting and importing of various parameters, which are formed in other layers. In our system, we are interested to use the cross-layer design to import security/QoS-related parameters at the application layer, which are used for proper encoder (voice and video) quality tunings. In this cross-layer technique, we gather parameters from three different layers, including:

Physical layer: The *RSSI* (*Received Signal Strength Indicator*) indicates the strength of the Access Point (AP) signal. It is represented by dBm. The range is between −94 dBm up to −30 dBm. We can show this parameter with 6 bits (64 different values).

Signal to noise ratio (SNR) shows the relative ratio between the sender signal power to the noise level. This indicator is important because the higher the SNR value, the higher the bandwidth can get. We can show this value with 7 bits (128 different values).

MAC layer: The *WMM* (*Wireless Multimedia*) is a three bit MAC layer QoS schemes used in Wi-Fi systems (IEEE 802.11e). Other types of MAC layer QoS metrics can often be translated to WMM. For instance wired MAC layer QoS scheme; IEEE 802.11p and IEEE 802.11Q, are also based on bits, which can be translated to WMM one-to-one.

Network layer: IP header (network layer) includes the field *DSCP* (*Differentiated Services Code Point*), which is an 8-bit field. Not all vendors configure all 8 bits, however the first 3 bits, which are configured by most vendors are called "Class Selector". In this case the rest of the 5 bits are left clear. Some vendors easily translate the Class Selector bits into WMM 3 bit values one-by-one. However we take the whole 8 bits. Therefore the *Cross-Layered Parameters* (*CLPs*) bits are: 7 + 6 + 3 + 8 = 24 bits.

The CLPs are checked by both sender and receiver encoder/decoder to adapt to the best possible coding rates. High quality indications of the CLPs can inform the application layer that the user requires high quality encoding. This may also be due to the fact that the medium is able to handle high throughput requirements. In bad channel conditions, CLPs point to low values, which triggers a lower encoding quality, which in term inform the application layer accordingly to avoid possible uneven drop of performance.

Now that the data handling at the application is complete, the processed information, including (Fig. 3): hash, cross-layer, digital signature, and the multimedia information are sent to the transport layer.

5. Transport, network, MAC, and PHY layers data handling

Once data is passed from the application layer to the transport layer, UDP starts shaping the incoming information into its payloads. Fig. 4 shows the hierarchy of functions and data handling procedures. UDP is the main transport protocol conveying the payload (i.e., hash, cross-layer, digital signature, and multimedia information).

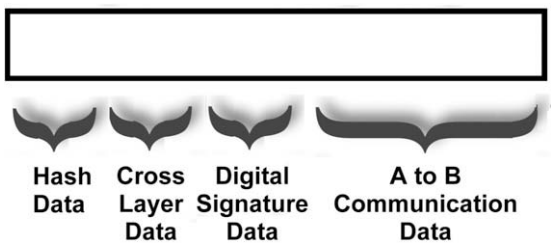

Fig. 3. Application layer functions.

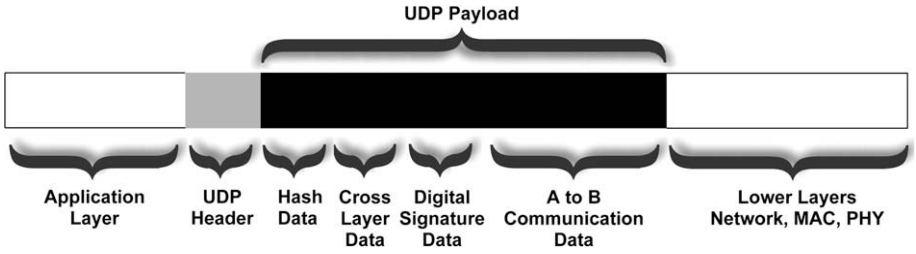

Fig. 4. Application, transport, network, MAC, and PHY layers processing hierarchy.

The network layer is responsible for three main functions; providing remote internetwork address (IP address), the routing QoS (IP-DSCP), and the routing security (IPSec).

There are two flavors of IPSec mechanism (Shaikh and Al-Khayatt, 2004); Authentication Header (AH) and Encapsulating Security Payload (ESP). An AH scheme provides hashing and data authentication mechanisms without encryption. Therefore AH-IPSec messages can be viewable by a third party.

An ESP scheme also comes in two flavors; Tunnel mode and Transport mode. In tunnel mode, the IP header (e.g., source and destination addresses) is encrypted in addition to what AH provides. Therefore in tunnel mode, headers require frequent decryptions/re-encryptions passing through each node and hub for routing purposes.

For our purpose, IPSec (ESP) is used to encrypt the entire IP payload and as a consequence, the entire UDP payload will be encrypted as well (Shaikh and Al-Khayatt, 2004). Fig. 5 (adapted from Shaikh and Al-Khayatt (2004)) shows the IPSec packet level representations for both tunnel and transport modes.

Following network layer data handling, MAC and PHY layers are next in the system hierarchy. Various IEEE standards are used at these two layers; IEEE 802.11i is used to address both MAC and PHY layer requirements, using WEP (64/128 bits) Hong and Lemhachheche, 2003, WPA-TKIP (d'Otreppe de Bouvette, 2008), or WPA-AES (Gruenauer, 2005). We will consider the effects of the deployments of these security protocols on the overall performance in the next section.

6. Multi-layer detailed system design

6.1. Application layer

The main communication protocols conveying digital ID, CLPs, and other information is UDP, which operates on top of IP. Besides the digital ID and the CLPs, two parties will be communicating in the following formats:

Text: This can be non-interactive (email) or interactive (text-chat). In this case, keyboard key strokes are captured and placed in the UDP payload along with CLP and digital ID.

Interactive typing requires a very low bandwidth. An average professional typist reaches 50–70 words per minute (WPM), usually less than 100 WPM. Therefore an interactive (two-way) typing session transmitting 100 + 100 = 200 WPM (for full-duplex PHY/MAC services) will require about 4 WPM, which requires less than 40 bps. In terms of the UDP payload per packet, this translates to only one byte of information per communication instance.

Voice: This is usually an interactive VoIP call or a normal voice-chat. In both cases, voices are captured and coded into a voice codec, such as G.711, and packed into the UDP payload. G.711 packets run at 64 kbps. A typical G.711 packet runs for 30 ms with a payload of 240 bytes; (240 bytes $\times$ 8 bits)/30 ms = 64 kbps.

Video: This is also an interactive videoconferencing communication between two (point-to-point) or more parties (multicasting). Video is often accompanied by voice and text. In this case, one of the well-known video codec; H.262, H.263, or H.264 could be used. All three mentioned codecs could be running at the minimum rate of 64 kbps.

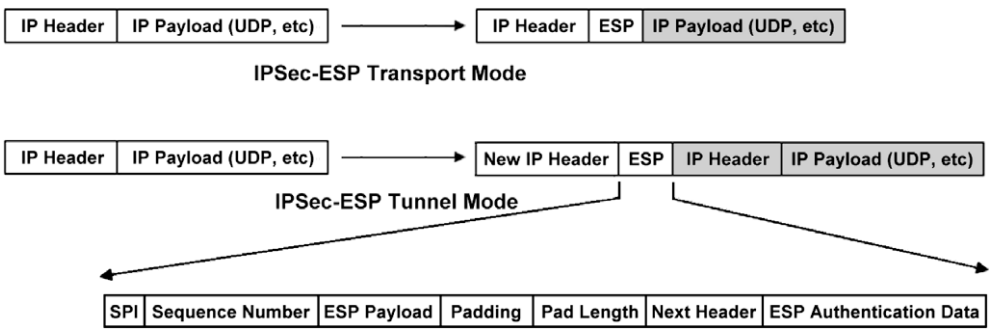

Fig. 5. IPSec-ESP packets (transport and tunnel modes).

Table 4
G.711 and H.264 codec datasheet.

Codec	Minimum bit rate	Resolution	Codec delay	Packet time interval	Bytes per packet
G.711	64 kbps	8 bits	0.25 ms	30 ms	240 bytes
H.264/MPEG-4	64 kbps	177 × 144 pixels 15 fps (QCIF)	7.36 ms/frame	66 ms	542 bytes

H.264, which is a newer and preferred codec, compared H.263 and H.262, is able to transport video information starting from 15 fps (frame per seconds) at 177 × 144 (QCIF) resolution. H.264 (similar to MPEG-4) often uses RTP (Real Time Transport Protocol (Wenger et al., 2005). H.264 requires approximately 6500 bits per frame (Zhihai et al., 2001; Zhang et al., 2009) with a minimum 10 ms of frame size (Nemethova et al., 2007), which results 65,000 bits per second (inline with the 64 kbps requirement). There are 15 fps with 66 ms inter-frame delays, which will results 15 packets per second with each containing 542 bytes of H.264.MPEG-4 encoded video information (Table 4). The codec delays are measured based on Acer TravelMate 4020 with Pentium M 725, 1.6 GHz, 400 MHz FSB, and 256 MB RAM platform.

The combination of RTP (12 bytes)/UDP (8 bytes)/IP (20 bytes) adds a minimum of 40 bytes overhead for the header.

6.1.1. Digital signature (DSA and RSA)

In this section, we will study the details of the mechanism featuring one of the two digital signature methods; DSA and RSA. The DSA scheme is based on Digital Signature Standard (DSS), proposed by NIST (National Institute of Standards and Technology) and published by FIPS (Federal Information Processing Standard) PUB (publication) 186-x. The hash size of DSA is 160 bits and the signature length of DSA is 40 bytes or 320 bits.

For the same platform, a DSA-1024 scheme would require 3.8 ms time for signing and 4.6 ms time for verifying (Yin et al., 2007; Riedel, 2003).

The RSA-1024 scheme, on the other hand, produces a 128 bytes (1024 bits) signature and requires 6.8 ms for signing and 0.35 ms for verifying (Niedermayer et al., 2006; Shaikh and Khayatt, 2004). Table 5 (adapted from Niedermayer et al. (2006)) represents the performance measures for RSA and DSA. The specifications and performance figures for SHA-1, -256, -512 are given in Table 6. The results in Tables 5 and 6 should be considered for performance evaluation of the system that transmits both digital signature and multimedia enriched information.

6.2. Transport layer

The only mechanism involved in this layer is UDP and since UDP is a transport mechanism and is not involved directly in the performance of the system, the UDP encapsulation/decapsulation delays are considered negligible.

Table 5
Performance measures for RSA and DSA.

DS scheme	Signature length (bytes)	Signing time (ms)	Verifying time (ms)	Total time (ms)
DSA-1024	40	3.8	4.6	8.4
RSA-1024	128	6.8	0.35	7.15

Table 6
SHA algorithms comparisons.

Hash function	Number of rounds	Hash size (bytes)	Block size (bytes)	Delay per block (ms)
SHA-1	80	20	64	2.6
SHA-256	64	32	64	3.4
SHA-512	80	64	128	9.04

Table 7
IPSec-ESP overhead.

ESP mode	Fixed portion (bytes)	Variable portion (bytes)	Total length (bytes)	Processing time
Transport mode	10	12	22	3DES: 0.152 ms AES-128: 0.0252 ms
Tunnel mode	30	12	42	3DES: 0.153 ms AES-128: 0.0256 ms

6.3. Network layer

IP and IPSec are the main protocols used in the network layer. Since these two schemes have direct impacts on the QoS and security measures, we will consider their performance measures in our calculations.

Table 7 (adapted from Limon Garcia (2008)) shows the overhead incurred for IPSec-ESP for both transport and tunnel modes on the same platform.

The existing benchmarks on IPSec performance are specified for (Limon Garcia, 2008; Siwamogsatham et al., 2008): Throughput, latency, frame loss rate, forwarding rates, and load sizes.

Fig. 6 (adapted from Limon Garcia (2008)) shows IPSec's normalized cryptographic performance for two different encryption schemes (AES and 3DES) versus packet sizes.

Fig. 7 (adapted from Limon Garcia (2008)) shows IPSec's delay figures for various packet sizes where latency decreases as the packet size increases. Packet sizes above 512 bytes exhibit relatively low latency figures compared to lower packet sizes.

Fig. 8 (adapted from Limon Garcia (2008)) shows IPSec's jitter figures for various packet sizes. Packet sizes close to 512 bytes and above 1400 bytes show relatively low jitter figures.

Fig. 9 (adapted from Limon Garcia (2008)) shows the IPSec's frame loss figures for different frame rates. As packet size increases, the frame loss figures also increase.

6.4. MAC/PHY layers

The main protocol impacting security at these layers, as mentioned, are based on the IEEE 802.11 standard (IEEE 802.11i), which include: WEP, WPA-PSK, WPA-TKIP, or WPA-AES.

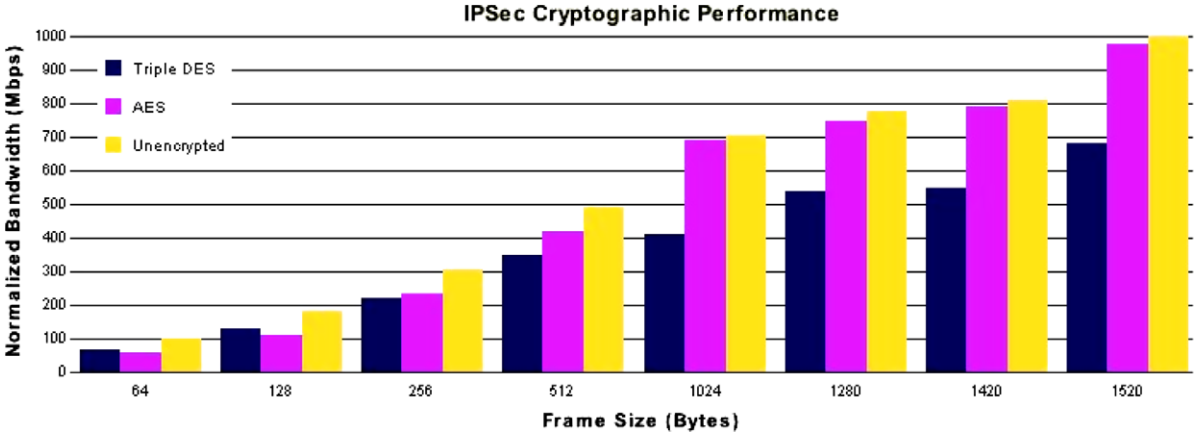

Fig. 6. IPSec cryptographic performance figures.

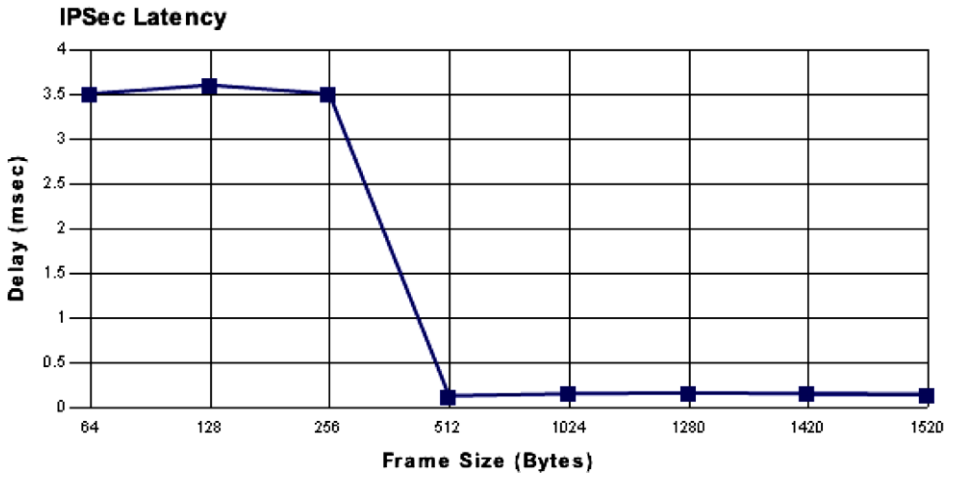

Fig. 7. IPSec's delay figures.

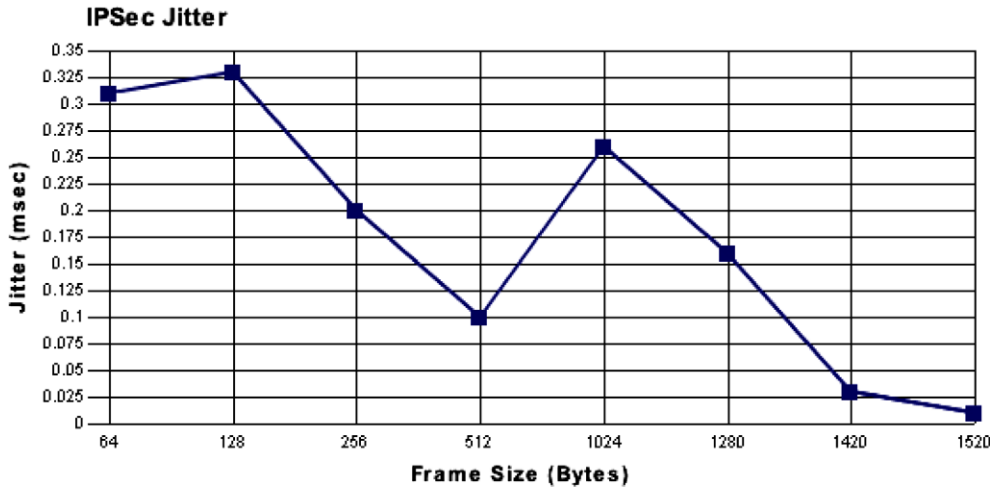

Fig. 8. IPSec's jitter figures.

Table 8 shows the performance comparisons between WEP, WPA-PSK-TKIP, and WPA-AES (Hong and Lemhachheche, 2003; Siwamogsatham et al., 2008), which shows that TKIP has the highest overhead of 160 bits. However this overhead in comparison to a frame with 1000 bytes long would be only 2%. The effect of encryption on the bandwidth is often negligible (around 1%).

7. QoS discussions

Table 9 gathers the summary of the system's performance measures in terms total payload and overhead. An observation while hashing is performed indicates that the delay figures given in Table 6 are delay per block, therefore to calculate the

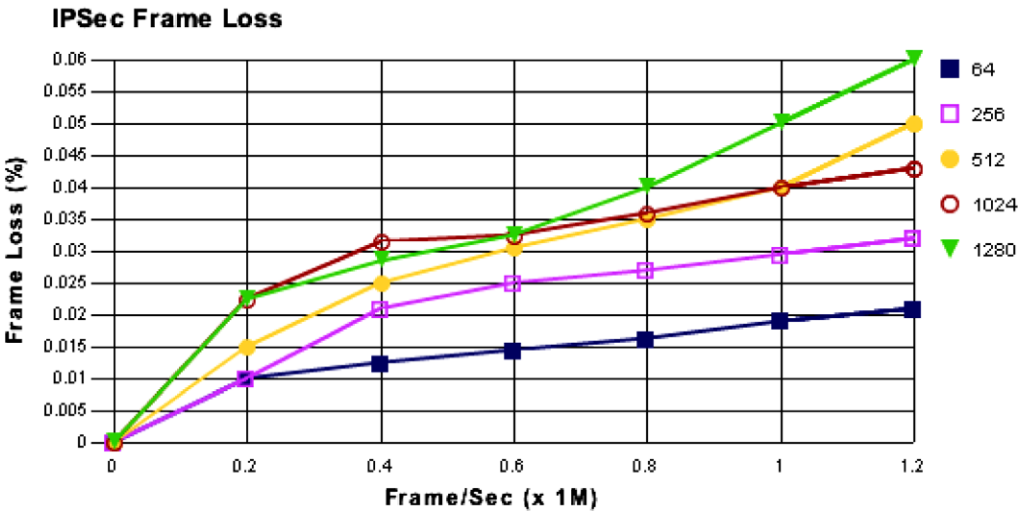

Fig. 9. Frame loss versus frame rates.

Table 8
Summary of WEP and WPA security methods.

Security method	Encryption algorithm	Number of Cipher keys	Overhead (bytes)
WEP (64 and 128)	RC4	64 (24 IV, 40 Keys) 128 (24 IV, 104 Keys)	24 + 8+32 = 64/8 = 8
WPA-PSK-TKIP	RC4	160 bits	20
WPA-AES	AES + CTR	128 or 256	16

Table 9
UDP's total payload size and time overhead variations with hashing (One Way).

Cross-layer information (bits)	Digital signature type	Party A to Party B communication type	Hashing Method	Total Payload (bytes)	Overhead (ms)
24	DSA	Text	SHA-1	72	6.40
			SHA-256	84	7.20
			SHA-512	116	12.84
		Voice	SHA-1	311	17.05
			SHA-256	323	21.05
			SHA-512	355	31.17
		Video	SHA-1	613	37.16
			SHA-256	625	45.16
			SHA-512	657	56.36
		Text + VO + VI	SHA-1	854	47.81
			SHA-256	864	59.01
			SHA-512	898	74.69
	RSA	Text	SHA-1	160	14.60
			SHA-256	172	17
			SHA-512	204	24.88
		Voice	SHA-1	399	22.65
			SHA-256	411	27.45
			SHA-512	443	34.17
		Video	SHA-1	701	42.76
			SHA-256	713	51.56
			SHA-512	745	68.40
		Text + VO + VI	SHA-1	942	53.66
			SHA-256	954	65.66
			SHA-512	986	86.98

total amount of delay overhead, one has to find the total number of blocks in which the hashing algorithm requires and multiple the value given in the delay per block column by the number of resulted blocks. For instance UDP payload with DSA and voice has a total of 291 bytes length. To derive the SHA-256 hash, there are five blocks of 64 bits, therefore according to Table 6, which states SHA-256 has delay per block of 3.4 ms, therefore for a payload of 291 bytes, there are 4.54 blocks of 64 bytes, rounding up to 5 blocks. Therefore the delay incurred by SHA-256 alone is 5×3.4 ms = 17 ms and the total amount of delay will be 4.05 + 17 = 21.05 ms.

This section also deals with the Labview experimental work using Labview 8.5. Labview is a system design software that is capable of generating real-time traffic based on graphical and visual block diagrams comprised of functional entities. These functional entities are programmed to perform certain tasks and/or deal with data in an algorithmic flow.

Table 10 shows three scenarios while both sender and receiver are directly connected to the ports in a router. Since wireless networks are bypassed, the mentioned average values for delay, jitter, and throughput figures are expected to be higher than values for IEEE 802.11-based traffic.

Table 11 includes the same parameters, however on an open access IEEE 802.11 (no security), instead of a wired network.

Table 12 presents the same parameters, however on a WEP-based IEEE 802.11 access network.

Tables 13 and 14 show the same results on WPA-PSK and WPA-AES networks.

Table 10
Experimental performance results in a wired Network.

Digital signature scheme	Multimedia UDP payload	Hashing method	Average E2E delay (ms)	Average received jitter (ms)	Average received throughput (kbps)
None	None	None	2.15	1.05	6.24
DSA	Voice	None	9.23	4.22	4.65
RSA	Vo + Vi + Text	SHA-512	169.55	66.40	3.12

Table 11
Experimental performance results in an open access IEEE 802.11 Network.

Digital signature scheme	Multimedia UDP payload	Hashing method	Average E2E delay (ms)	Average received jitter (ms)	Average received throughput (kbps)
None	None	None	3.23	1.26	4.14
DSA	Voice	None	10.44	4.89	3.86
RSA	Vo + Vi + Text	SHA-512	172.34	69.24	2.34

Table 12
Experimental performance results in a WEP-based IEEE 802.11 Network.

Digital signature scheme	Multimedia UDP payload	Hashing method	Average E2E delay (ms)	Average received jitter (ms)	Average received throughput (kbps)
None	None	None	12.24	4.56	4.05
DSA	Voice	None	19.73	7.22	3.78
RSA	Vo + Vi + Text	SHA-512	179.23	74.46	2.28

Table 13
Experimental performance results in a WPA-PSK-based IEEE 802.11 Network.

Digital signature scheme	Multimedia UDP payload	Hashing method	Average E2E delay (ms)	Average received jitter (ms)	Average received throughput (kbps)
None	None	None	12.09	4.43	3.99
DSA	Voice	None	19.43	7.09	3.72
RSA	Vo + Vi + Text	SHA-512	178.63	73.57	2.24

Table 14
Experimental performance results in a WPA-AES-based IEEE 802.11 Network.

Digital signature scheme	Multimedia UDP payload	Hashing method	Average E2E delay (ms)	Average received jitter (ms)	Average received throughput (kbps)
None	None	None	12.05	4.33	4.04
DSA	Voice	None	19.39	7.02	3.76
RSA	Vo + Vi + Text	SHA-512	178.44	73.24	2.26

Table 15 shows the three cases for which performance graphs are created. These cases are: Case 1). No digital signature, no hash function, and only text messages. Case 2). DSA-1024, no hash function and only voice messages. Case 3). RSA-1024, SHA-512, and all three (voice, video, and text) messages. Figs. 10 and 11 shows the end-to-end (two-way) performances of these three cases and Fig. 12 shows the end-to-end performance comparison results between theoretical and experimental results.

Table 15
The three scenarios used in the experimental result.

Case	Digital signature	Hash function	Multimedia payload
Case 1	–	–	Text
Case 2	DSA	–	Voice
Case 3	RSA	SHA-512	Text + Voice + Video

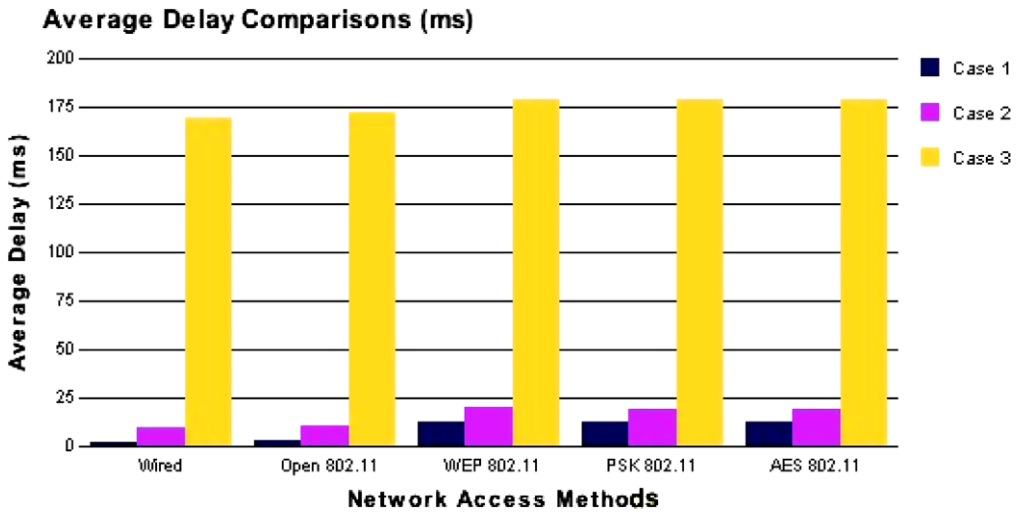

Fig. 10. Experimental results for the wireless network access average delays.

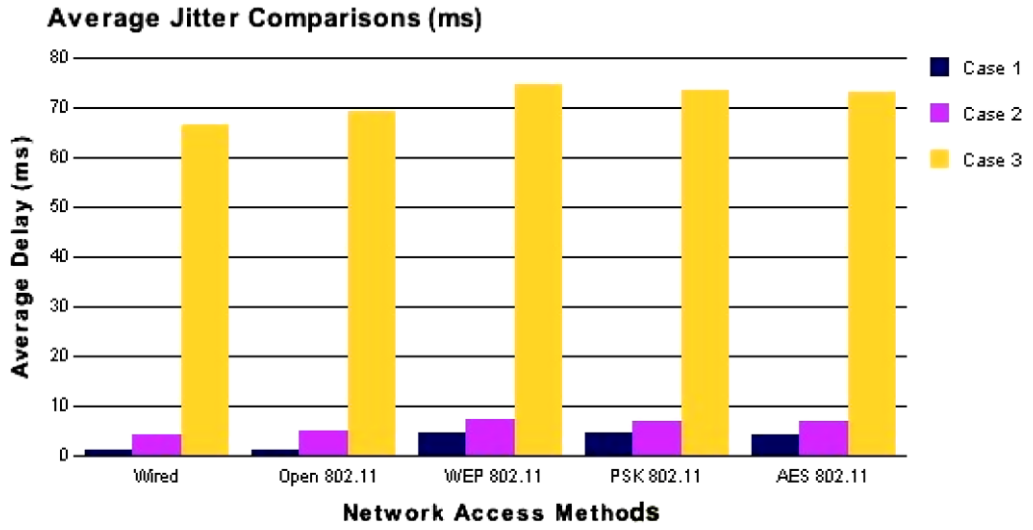

Fig. 11. Experimental results for the wireless network access average jitters.

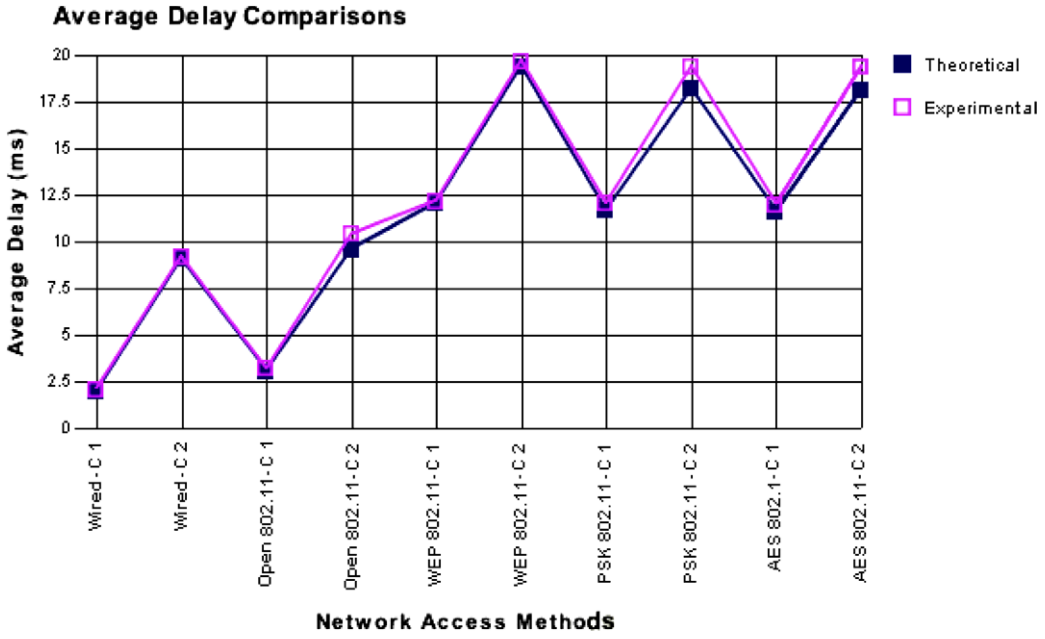

Fig. 12. Experimental and theoretical results comparisons.

Fig. 12 compares the experimental results to the theoretical results for the two cases (C1 and C2), which shows a very tight match between these two sets of results. The highest error value was observed in C2 on AES access network where we have 6.5% error between the experimental and theoretical results.

8. Security analysis

Table 16 summarizes the security summary of the entire system. It includes the algorithms used in each layer and to point to the fact that the specific algorithm is either vulnerable or secure. With appropriate selections (based on AES), both network and MAC layers can be considered as secure and the rest of the layers may have security vulnerabilities. There are remedies listed for each security weakness, however depending on the scenarios, the remedies may or may not be conclusive. Denial of Service (DoS) attack is the main issue at the physical layer, which can be dealt with using DoS deterrence proce-

Table 16
System layered security analysis summary.

Layers	Algorithm or mechanisms	Vulnerable/ secure	Security weaknesses	Remedy
Physical	Air, Database or Local Drive	Vulnerable	Unauthorized access, DoS, tapping,	DoS attack deterrence
MAC	IEEE 802.11 – WEP	Vulnerable	Easily hacked	Dynamic WEP/ WPA
	IEEE 802.11 (WPA-TKIP)	Vulnerable	Breakable	WPA-AES
	IEEE 802.11 – WPA-AES	Secure	–	–
Network	IPSec-AH	Vulnerable	No encryption	IPSec-ESP
	IPSec-ESP	Secure	–	–
Transport	UDP	Vulnerable	Port scan, flooding, session hijack, traffic analysis	SSL, TLS, NTLP, SCTP
Application	Voice authentication, Hash, Digital Signature (RSA/DSA)	Vulnerable	Birthday Attack	SHA-256, 384, 512 DSA-2048 RSA-2048

dures. WEP-based MAC services are proved to be flawed. Switching to dynamic WEP may increase the security strength to some limits or choosing WPA-AES is ultimately the best MAC layer solution. At the network layer, IPSec - ESP based on AES is the best solution in terms of security strength at the network layer. We have not considered any security schemes at the transport layer, relying on both the security at the application and network layers to compensate. However there are a few security solutions available for this layer, including: Secure Sockets Layer (SSL), Transport Layer Security (TLS), NSIS (Next Steps In Signaling) Transport Layer Protocol (NTLP) and Stream Control Transmission Protocol (SCTP).

A multi-layer approach is often needed to provide a more solid security capability to the system.

9. Conclusion

In this paper we studied the security requirements of m-learning systems and developed an application layer non-repudiation system based on a person's biometric information, which resulted in the generation of a digital ID. These IDs were based on certain biometric characteristics and were uniquely created for each user and then digital signatures were created based on the digital IDs. In parallel, three cross-layer-based parameters were extracted from the cross-layer system and imported to the application layer and the application layer encoder used these parameters for proper encoding quality adjustment. A hash function was utilized and applied to the entire data payload (digital ID, cross-layer information, generated digital signature, and the multimedia data), and the resulted hash value was added to the pre-hashed payload and the entire information was packed in the UDP (User Datagram Protocol) payload.

The performance of the system can be studied based on the overhead, average time delays, average received jitter values, and average throughput values. We performed a thorough comparison study based on the delay figures, which includes a theoretical performance evaluation, comparing the theoretical results to the experimental results based on the outputs generated by Labview 8.5 transmitter/receiver testbeds. The results showed that the experimental results matched the theoretical values with a maximum of 6.5% error. This means that the designed system was able to maintain high QoS- and security-related performances while offering acceptable end-to-end delay/jitter and bandwidth figures.

We also presented the security analysis in a table and discussed the vulnerabilities and the remedy schemes.

The direction of the future work includes cellular-based testbeds on 2G and 3G networks instead of Wi-Fi access technologies and repeat the same experimental tests and compare the results.

Acknowledgement

This work was supported in part by the Natural Sciences and Engineering Research Council of Canada.

References

Anwar, M., Greer, J., 2006. Reputation Management in Privacy-Enhanced E-learning. In: Proceedings of the 3rd Annual Scientific Conference of the LORNET Research Network (I2LOR-06), Montreal, Canada, November 2006.

Arjona, A., Verkasalo, H., 2007. Unlicensed Mobile Access (UMA) Handover and Packet Data Performance Analysis. In: Second International Conference on Digital Telecommunications (ICDT 2007), 1–5 July 2007.

Bandwidth Calculator for VOIP. AsteriskGUIDE, 2006. <http://blog.asteriskguide.com/bandcalc/bandcalc.php>.

Bechelli, L., Bistarelli, S., Martinelli, F., Petrocchi, M., Vaccarelli, A., 2002. Integrating Biometric Techniques with an Electronic Signature for Remote Authentication. In: European Research Consortium for Informatics and Mathematics (ERCIM 2002), vol. 49, April 2002.

Camarillo G. Session Description Protocol (SDP) Format for Binary Floor Control Protocol (BFCP) Streams, RFC 4583, November 2006. <http://www.ietf.org/rfc/rfc4583.txt>.

Camarillo, G., Eriksson, G., Holler, J., Schulzrinne, H. Grouping of Media Lines in the Session Description Protocol (SDP), RFC 3388, December 2002. <http://www.ietf.org/rfc/rfc3388.txt>.

Camarillo, G., Ott, J., Drage, K. The Binary Floor Control Protocol (BFCP), RFC 4582, November 2006. <http://www.ietf.org/rfc/rfc4582.txt>.

Cavoukian, A., Stoianov, A., 2007. Biometric Encryption: A Positive-Sum Technology that Achieves Strong Authentication, Security AND Privacy, March 2007. <http://www.ipc.on.ca/images/Resources/up-1bio_encryp.pdf>.
Diab, W.B., Tohme, S., Bassil, C., 2008. VPN Analysis and New Perspective for Securing Voice over VPN Networks. In: Fourth International Conference on Networking and Services (ICNS 2008), Gosier, Guadeloupe, March 16–21, 2008, pp. 73–78.
Digital Signature Algorithm, 2009. Wikipedia, Retrieved on May 23rd, 2009. <http://en.wikipedia.org/wiki/Digital_Signature_Algorithm>.
d'Otreppe de Bouvette, T., 2008. WPA, what else? Aircrack-ng, UNAM, Mexico City, November 27–28, 2008. <http://intromision.fciencias.unam.mx/1_UNAM_08.ppt>.
Electronic Learning, 2009. Wikipedia, Retrieved on May 21st, 2009. <http://en.wikipedia.org/wiki/Electronic_learning>.
Gruenauer, J., 2005. Wireless network security standard, June 2005. <http://joerg.gruenauer.doesntexist.org/WLANSecurity_V2.ppt>.
H.239, Wikipedia, retrieved on May 20th 2009. <http://en.wikipedia.org/wiki/H.239>.
Hautakorpi, J., Camarillo, G. The Session Description Protocol (SDP) Content Attribute, RFC 4796, February 2007. <http://tools.ietf.org/html/rfc4796>.
Hinard, Y., Bettahar, H., Challal, Y., Bouabdallah, A. Layered multicast data origin authentication and non-repudiation over lossy networks, ISCC'06. In: IEEE Symposium on Computers and Communications, 2006, Pula-Cagliari, Italy.
Hong, J., Lemhachheche, R., 2003. WEP Protocol Weaknesses and Vulnerabilities. ECE 578: Computer & Network Security Research Project, Spring 2003.
IEEE 802.11e-2005, 2009. Wikipedia, Retrieved on May 23rd, 2009. <http://en.wikipedia.org/wiki/802.11e>.
IEEE 802.11i-2004, 2009. Wikipedia, Retrieved on May 23rd, 2009. <http://en.wikipedia.org/wiki/802.11i>.
Karapetkov, S. UC driving protocol convergence: the road to SIP visual communications is paved with challenges—and benefits—for end-users, July 2008, Retrieved on May 20th, 2009. <http://findarticles.com/p/articles/mi_m0CMN/is_7_45/ai_n29475477/>.
Kritzinger, E., von Solms, S.H., 2006. E-learning: Incorporating Information Security Governance. In: Issues in Informing Science and Information Technology Conference (InSITE 2006), Salford, England, 2006.
Levin, O., Camarillo, G. The Session Description Protocol (SDP) Label Attribute, RFC 4574, August 2006. <http://www.ietf.org/rfc/rfc4574.txt>.
Limon Garcia, G., 2008. IPSec performance analysis for large-scale Radio Access Networks. Master Thesis, July 2008. <http://www.tkk.fi/Units/CSE/NordSecMob/Thesisworks/Thesis_GabrielaLimon_TKK.pdf>.
Living List of Identity Management Terminology, ITUwiki, 2009. Retrieved on May 22nd, 2009. <http://www.ituwiki.com/index.php?title=Living_List_of_Identity_Management_Terminology>.
Markendahl, J., Makitalo, O., Werding, J., 2008. Analysis of Cost Structure and Business Model options for Wireless Access provisioning using Femtocell solutions. In: 19th European Regional ITS Conference Luiss Guido Carli University, Rome, 18–20 September 2008.
MLearning, 2009. Wikipedia, Retrieved on May 22nd, 2009. <http://en.wikipedia.org/wiki/M-learning>.
Nemethova, O., Karner, W., Rupp, M., 2007. Error Prediction Based Redundancy Control for Robust Transmission of Video over Wireless Links, ICC 2007.
Nesimoglu, T., Parker, S.C.J., Morris, K.A., McGeehan, J.P. The performance and efficiency of envelope elimination and restoration transmitters for future multiple-input multiple-output wireless local area networks. In: IET Communications, vol. 2 (3), March 2008.
Nickolova, M., Nickolov, E., 2007. Threat Model for User Security in E-Learning Systems. In: International Journal on Information Technologies and Knowledge, vol. 1, 2007.
Niedermayer, H., Klenk, A., Carle, G., 2006. The Networking Perspective of Security Performance – A Measurement Study, MMB 2006.
Park, K.W., Seok, H., Park, K.H., 2007. pKASSO: Towards Seamless Authentication Providing Non-Repudiation on Resource-Constrained Devices. In: Proceedings 21st IEEE International Conference Advanced Information Networking and Applications Workshops, vol. 2, 2007, pp. 105–112.
Pérez-Costa, X., Vidal, A., Camps-Mur, D., 2006. SU-APSD: Static IEEE 802.11e Unscheduled Automatic Power Save Delivery. In: European Wireless Conference (EW), Athens, Greece, April 2006.
Raitman, R., Ngo, L., Augar, N., Zhou, W., 2005. Security in the online e-learning environment. In: Proceedings of 5th IEEE International Conference on Advanced Learning Technologies (ICALT 2005), 5–8 July, 2005, Kaohsiung, Taiwan.
Riedel, I., 2003. Security in Ad-hoc Networks: Protocols and Elliptic Curve Cryptography on an Embedded Platform. Diploma Thesis, Ruhr-University of Bochum, March 2003.
RSA, 2009. Wikipedia, Retrieved on May 23rd, 2009. <http://en.wikipedia.org/wiki/RSA>.
SHA hash functions, Wikipedia, Retrieved on May 23rd, 2009. <http://en.wikipedia.org/wiki/SHA_hash_functions>.
Shaikh, S.A., Al-Khayatt, S.A., 2004. A Performance Study of IPSec Protocol. In: International Conference on Information and Computer Science (ICICS'04).
Siwamogsatham, S., Srilasak, S., Limmongkol, K., Wongthavarawat, K., 2008. Encryption vs. Performance of Infrastructure IEEE 802.11 WLANs. Wireless Telecommunications Symposium (WTS 2008), 24–26 April 2008, pp. 405–408.
Stach, J.F., Park, E.K., 1998. Analysis of a Non-repudiation Authentication Protocol for Personal Communication Systems. In: Proceedings of 1998 IEEE International Conference on Computer Communications and Networks, Lafayette, Louisiana, October 1998, pp. 289–293.
Stoianov, A., 2008. Biometric Encryption: Emerging Privacy-Enhancing Technologies. Ontario Government Access & Privacy Workshop, October 7, 2008. <http://www.verney.ca/onapw2008/presentations/660.pdf>.
Topiwala, P., Jindal, M., 2004. H.264/AVC: Overview and Intro to Fidelity-Range Extensions, FastVDO, 2004. <http://www.ti.com/asia/docs/india/tiidevconf2004/analog_symp/munish.pdf>.
Video Conferencing Standards, Tandberg, Application Notes, D10740, Rev 2.3, Retrieved on May 23rd, 2009. <http://www.tandberg.com/collateral/white_papers/whitepaper_Videoconferencing_standards.pdf>.
Voice Over IP – Per Call Bandwidth Consumption, Cisco Systems, Document ID: 7934, February 2006. <http://www.cisco.com/en/US/tech/tk652/tk698/technologies_tech_note09186a0080094ae2.shtml>.
VoIP Bandwidth Calculation, Newport Networks, 2005. <http://www.newport-networks.com/whitepapers/voip-bandwidth3.html>.
Web 2.0, 2009. Wikipedia, Retrieved on May 22nd, 2009. <http://en.wikipedia.org/wiki/Web_2.0>.
Weippl, E., Ebner, M., 2008. Security & Privacy Challenges in E-Learning 2.0. In: Proceedings of E-Learn 2008, Las Vegas, p. 4001–4007.
Wenger, S., Hannuksela, M.M., Stockhammer, T., Westerlund, M., Singer, D. RTP Payload Format for H.264 Video, RFC 3984, February 2005. <http://www.rfc-editor.org/rfc/rfc3984.txt>.
Wiegand, T. Video Coding Standards, Digital Image Communication, 2007. <http://iphome.hhi.de/wiegand/assets/pdfs/DIC_video_coding_standards_07.pdf>.
Wi-Fi Protected Access, 2009. Wikipedia, Retrieved on May 23rd, 2009. <http://en.wikipedia.org/wiki/Wi-Fi_Protected_Access>.
Wired Equivalent Privacy, 2009. Wikipedia, Retrieved on May 23rd, 2009. <http://en.wikipedia.org/wiki/Wired_Equivalent_Privacy>.
Yin, H., Sheng, B., Wang, H., Pan, J., 2007. Securing BGP through Keychain-based Signatures. In: Fifteenth IEEE International Workshop on Quality of Service (IWQoS 2007), Evanston, IL, USA, June 21–22, 2007.
Yong, J., 2007. Security modeling for e-Learning. In: Proceedings of the 2007 1st International Symposium on Information Technologies & Applications in Education (ISITAE 2007), Kunming, China, pp. 1–5.
Zhang, X., Peng, X.H., Wu, D., 2009. A Hierarchical Unequal Packet Loss Protection Scheme for Robust H.264/AVC Transmission. In: Proceedings of the 6th Annual IEEE Consumer Communications & Networking Conference (CCNC 2009) UASS workshop, Las Vegas, Nevada, USA, January 10–13, 2009.
Zhao, J., Guo, Z., Zhu, W., 2003. Power Efficiency in IEEE 802.11a WLAN with Cross-Layer Adaptation. IEEE ICC 2003, 2003.
Zhihai, H., YongKwan, K., Sanjit, K.M., 2001. Object-level bit allocation and scalable rate control for MPEG-4 video coding. In: Proceedings of Workshop and Exhibition on MPEG-4, 2001.

Sasan Adibi (BS'95, MS'99, MS'05) is a Ph.D. student in his final semester at the Electrical and Computer Engineering Department of the University of Waterloo, Canada. His current research interests include; security and Quality of Service (QoS) in wireless technologies.