Design of a Secured Multimedia Transmission Scheme over Heterogeneous Wireless Systems

Md. Rakibul Islam[1], Preeti Bharti[2], Ronnie D. Caytiles[3]*

Abstract: The evolution of wireless technologies has paved the way for the massively increasing availability of multimedia content in all forms from the Internet. Wireless networks consist of heterogeneous and overlapping coverages of multiple access technologies. The transmission of multimedia contents in the open wireless network system such as the Internet will always be vulnerable to security threats and possible adversary attacks. This paper deals with the analysis and design of a robust transmission security scheme capable of protecting the handshake of devices over heterogeneous wireless systems. It incorporates the features of both symmetric and asymmetric encryption schemes to ensure and guarantee a secured multimedia content transmission.

Keywords: Multimedia, Secured transmission, Heterogeneous wireless system, Encryption scheme

1. Introduction

Multimedia contents may refer to the integration of different contents such as text, images and graphics, videos, audio, and animations and may come in different applications (*e.g.*, medical and healthcare applications, military databases, courseware, games, shopping applications, advertisements, videos on demand (VoDs), and various mobile applications). Such multimedia contents require not only the extensive processes of coding, storage, and distribution but also effective and robust transmission security without sacrificing its seamless delivery. Multimedia services transmission security can be essentially important in critical applications as its delivery will be through the open network systems such as the Internet.

Currently, various efforts have been developed for the integration and cooperation of different wireless network systems in order to provide seamless multimedia services. Numerous transmission protocols were optimized to provide reliable and continuous multimedia services over heterogeneous wireless systems. However, multimedia transmission over these overlapping heterogeneous wireless

[1] Multimedia Engineering Department, Hannam University, Daejeon, South Korea
Email: rakibulrocky27@gmail.com
[2] Multimedia Engineering Department, Hannam University, Daejeon, South Korea
Email: 1112preeti@gmail.com
[3]* Multimedia Engineering Department, Hannam University, Daejeon, South Korea
Email: rdcaytiles@hnu.kr (Corresponding Author)

Received [August 10, 2020]; Revised [October 15, 2020]; Accepted [November 2, 2020]

Published by InnoCon Publishing
ISSN 2704-4440

systems also requires an extensive security mechanism in order to ensure confidentiality, integrity, availability, authentication, and non-repudiation principles.

This paper deals with the analysis and design of an efficient and robust security scheme for the transmission of multimedia services over heterogeneous wireless systems. It utilizes the features of various cryptography algorithms to ensure a secured multimedia service transmission. Both symmetric and asymmetric encryption schemes were analyzed and incorporated to provide robustness of the security scheme.

The rest of this paper is organized as follows: Section 2 provides a discussion of the related literature wherein some existing security features of wireless network protocols have been outlined; the overview of the different encryption schemes was outlined in Section 3; the analysis and design of robust and secured multimedia services transmission over heterogeneous wireless systems is presented in Section 4; and the concluding remarks in Section 5.

2. Related Literature

Some protocol optimizations utilize pre-defined security features such as Wi-Fi Protected Access (WPA, WPA2), an encryption mechanism included in the IEEE 802.11 standards to secure wireless local area networks (WLAN). The WPA has been recommended to replace the security issues with the then wired equivalent privacy (WEP) mechanism. The WEP standard was considered as the most widely used Wi-Fi security protocol, but, numerous security limitations were found despite various revisions and enhancements. In this regard, the WPA was adapted by Wi-Fi Alliance to directly replace the WEP standard with its common configuration WPA-PSK (WPA Pre-Shared Key). Significant changes were made with the WPA standard as it uses 256-bit keys as compared to 64-bit and 128-bit keys that were used with the WEP. In addition, WPA includes message integrity checks in identifying whether adversaries have captured or modified the data packets that have been transmitted between wireless access links and client devices. Moreover, WPA also includes the Temporal Key Integrity Protocol (TKIP) that employs a per-packet keying system but was then replaced by the Advanced Encryption Standard (AES). Furthermore, some wireless access points offer Wi-Fi Protected Setup (WPS), which a quick way for a mobile device in joining an encrypted wireless network, but, nowadays, it is also no longer secure.

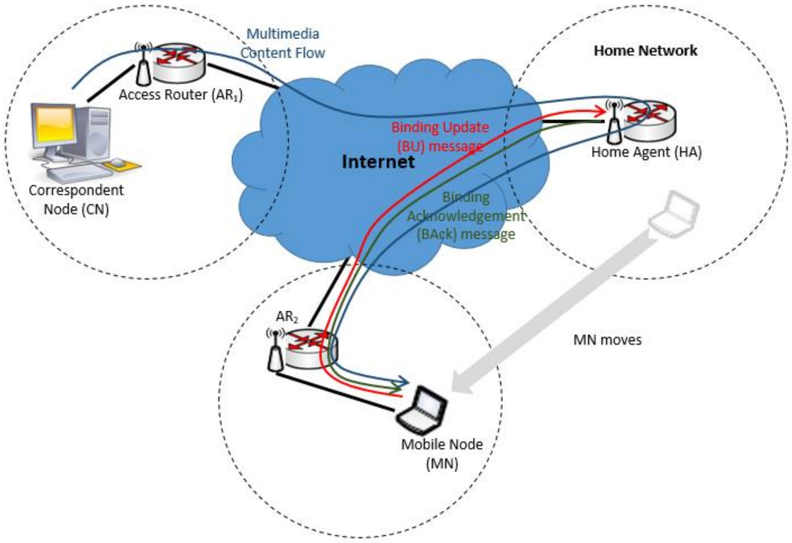
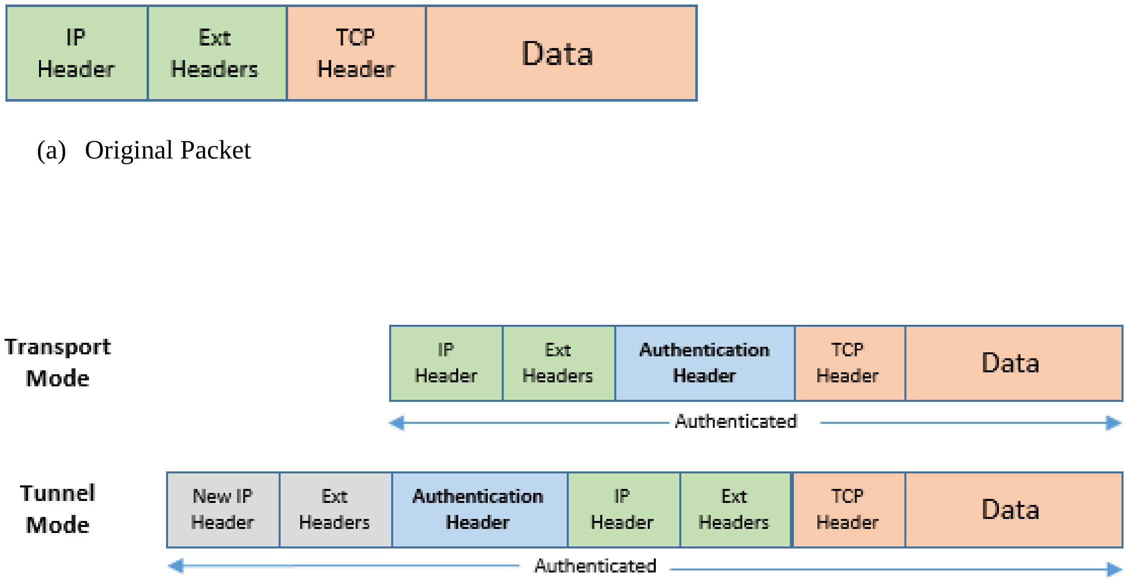


Figure 1. MIPv6 Basic Operations

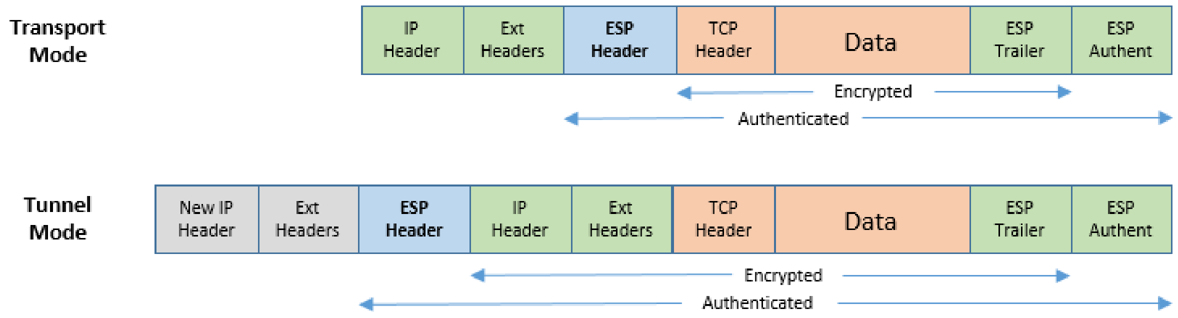
The mobile internet protocol version 6 (MIPv6) also utilizes various security features such as the utilization of Authentication Header (AH), Encapsulating Security Payload (ESP), IPSec modes, AH in Transport and Tunnel modes, and the Security Association (SA). The basic operation of MIPv6 is depicted in Figure 1 showing the movement of a mobile node (MN) from its home network to another network domain. The MN then sends a binding update (BU) message to its home agent (HA) to report its newly created Care-of Address (CoA) in addition to its permanent Home Address (HoA). The HA then sends back a binding acknowledgement (BAck) message to the MN as soon as it updates the MN's binding cache entry (BCE). After the exchange of binding messages, the HA intercepts all the packets intended for the MN's HoA and tunnels them to the MN's current CoA with proper encapsulations. The IPSec security is required in the IPv6 specification that enables packet authentication as well as an encryption of the packet payload through the utilization of extension headers. IPSec [1] allocate two security headers, the AH and ESP, which can be utilized separately or together in conjunction with the security key exchange. The AH provides connectionless integrity, authentication of the source of data, and protection against replay attacks [2]. In order to perform authentication, the Integrity Check Value (ICV) over the packet payload, the header, and the fixed fields on the MIPv6 header and options are calculated. The ESP in IPSec also provides the same features as the AH in connectionless integrity, authentication of the source of data, and protection against replay attacks, but in addition, it also provides limited traffic flow confidentiality, and privacy and confidentiality through packet payload encryption [2].

The IPSec [3][4] can utilize two different modes: (1) the transport mode (*i.e.*, host-to-host) wherein the original packet of MIPv6 header is followed by the AH or ESP header before the packet payload; (2) the tunnel mode *(i.e.*, gateway-to-gateway or gateway-to-host) wherein the new MIPv6 header will encapsulate the AH or ESP header and the original packet header and payload. The utilization of AH and ESP in both IPSec modes are depicted in Figure 2. In cases that both AH and ESP are utilized together, ESP must be applied first before the AH authenticates the entirety of the new packet. All other extension headers except for the destination options follow right immediately the IP header.



(a) Original Packet

(b) AH Header in both IPSec modes



(c) ESP Header in both IPSec modes

Figure 2. Utilization of AH and ESP in both Transport and Tunnel modes of IPSec

On the other hand, the SA refers to the record of the mode (transport or tunnel), authentication algorithm, encryption algorithm, keys being used, sequence number, overflow flag, SA expiration, and anti-replay window [5]. Each communication endpoint agrees with an SA which is held on a database and indexed by the outer destination address, the AH or ESP in the IPSec standard, and the Security Parameter Index value. SA selection can be manually using pre-shared keys or automatically through the use of Internet Key Exchange (IKE, IKEv2). The Diffie-Hellman techniques are used by the IKE in creating a shared secret encryption key used in SA data negotiations. The Public Key Infrastructure (PKI) on the other hand is used for key exchange for both IPSec modes wherein the syntax and framework refer to the Internet Security Association and Key Management Protocol (ISAKMP) [5].

- In the transport layer, the Transport Layer Security (TLS) and Secure Socket Layer (SSL) [6] were the cryptographic mechanisms that provide multimedia transmission security over network systems [7]. Such protocols were widely used in various applications such as electronic mails, messaging, web browsing, and voice over IP (VoIP). Providing privacy and data integrity for communication between two or more applications is the primary purpose of TLS. For example, using the TLS mechanism to secure the communication between the client application and a web server obtains the following principles [7]:
- Symmetric encryption for data packets being transmitted provides secure communication. The symmetric encryption keys are negotiated during the TLS handshake.
- Public-key cryptography will be required for one or both the web server and client application for authentication.
- Each transmitted packet includes a message integrity check that utilizes a message authentication code in order to prevent undetected loss or data modification during transmission making the connection reliable.

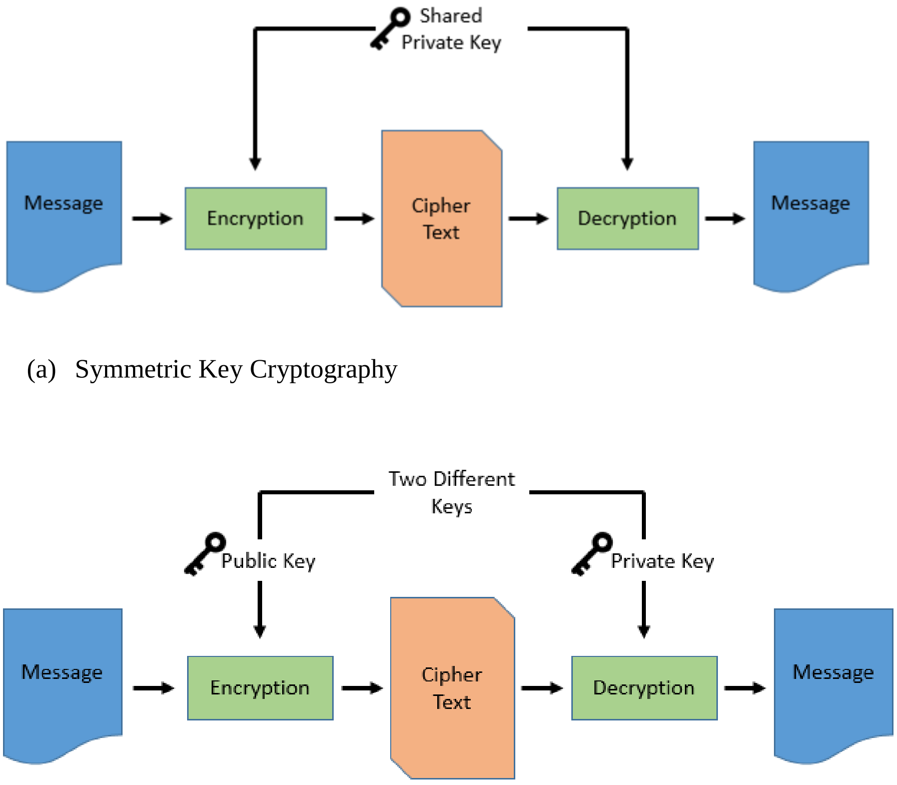
Another transport layer security mechanism is the use of SSL which becomes the standard security technique in establishing a secured link between a client application and a web server [6][8]. Data packet transmission in this encrypted link between the web server and client applications are assured with privacy and integrity. SSL connections have been widely used by websites to protect their online transactions specifically dealing with critical information such as credit card numbers, login credentials, and social security numbers.

The use of Secure Real-Time Protocol (SRTP) [9] in the transport layer also provides a secured communication specifically for VoIP communication. It utilizes both encryption and authentication schemes in order to prevent the risks of possible Denial of Service (DoS) attacks.

3. Analysis of Cryptography Algorithms

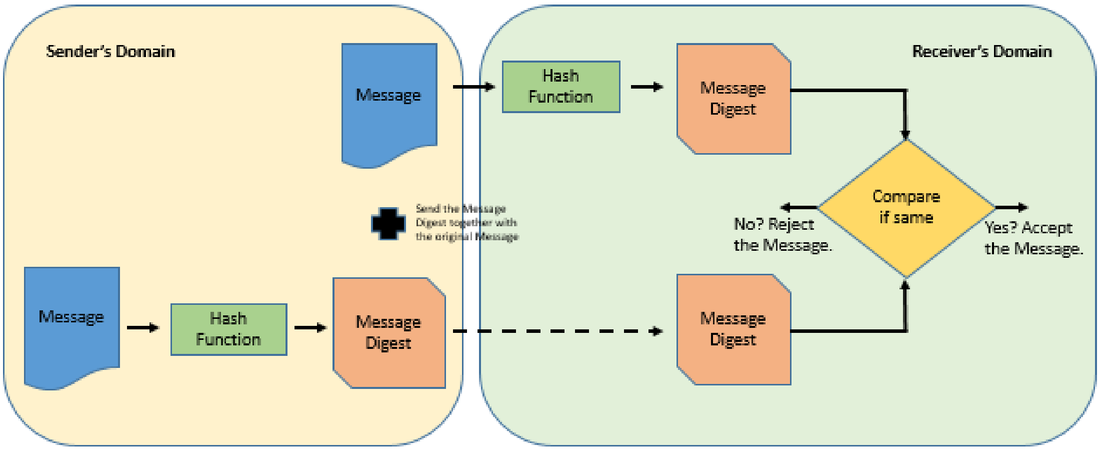
The transmission of multimedia services over open network systems requires a robust and explicit cryptography scheme to ensure its privacy and integrity. Cryptography means the utilization of techniques on securing data communications to prevent attackers to capture or alter transmitted messages [10]. It includes the analysis and construction of protocols that prevent the influence of attackers and are related to various security aspects of data confidentiality, integrity, authentication, availability, and non-repudiation. This section outlines the different encryption and security algorithms for utilization in the proposed design of the secured multimedia service transmission scheme.

The symmetric key cryptography shown in Figure 3(a) utilizes the same key to encrypt and decrypt data that are shared by both the communicating parties in securing a multimedia service transmission [11]. The same key must be shared and kept secret by both communicating parties during transmission. It provides data confidentiality and the algorithm process is faster as it only requires smaller size keys which are applicable in smaller-scale network systems. Symmetric key cryptography can be impractical to be applied in large-scale network systems as communicating parties are sharing the same keys for both encryption and decryption process wherein shared key distribution poses threats to be intercepted by attackers that can result to capture and alteration of critical information in multimedia services. Symmetric key algorithms generally use either stream or block ciphers [12]. The stream ciphers encrypt the digits or letters of a message one at a time (*e.g.*, Vigenere Cipher [13]). On the other hand, block ciphers encrypt a block of text in a message rather than encrypting one bit at a time. It utilizes a predetermined length key in order to create one block cipher (*e.g.*, Advanced Encryption Standard (AES) algorithm) [14].



(a) Symmetric Key Cryptography

(b) Asymmetric Key Cryptography



(c) Message Digest Algorithm

Figure 3. Cryptography Algorithms for the Secured Multimedia Content Transmission

Asymmetric encryption shown in Figure 3(b) also refers to public-key cryptography that utilizes public and private keys in performing its encryption and decryption processes. The paired keys are different from each other (*i.e.*, asymmetric) are comprised of large numbers. The public key can be shared openly with everyone, but the private key must be kept in secret and known only to the owner. For example, the sender can encrypt the message using the shared public key, but the message can only be decrypted using the receiver's private key. In addition, the message can be encrypted using a private key can be decrypted using the receiver's public key [15]. Public key cryptography is widely used in the open network communications such as the Internet. Common examples include the RSA (Rivest–Shamir–Adleman) algorithms, Digital Signature Algorithm (DSA), Elliptic Curve Cryptography (ECC) techniques, and Public-key cryptography standards (PKCS).

Message digests shown in Figure 3(c) refer to hash functions that are utilized in creating a shorter, fixed-length representation of a longer, variable-length message to be transmitted. The hash functions can be used in multimedia service transmission in order to enhance integrity by making it nonviable for the messages to determine from the digests. Two different messages that result in the same digest are impossible to find. Popular examples include MD5 message-digest algorithms and Secure Hash Algorithm (SHA) [16].

4. Design of Secured Multimedia Content Transmission

This paper deals with the analysis and design of a secured transmission of multimedia contents over heterogeneous wireless systems. Multimedia contents become susceptible to security threats and adversary attacks as its volume massively becomes available on the Internet. The transmission of such multimedia content over open networks is accompanied by higher risks of being captured and manipulated by adversaries for their own purposes [17]. In this regard, the combination of cryptography algorithms to safeguard possible adversary attacks has been designed as depicted in Figure 3.

The design of the secured multimedia contents transmission utilizes an asymmetric key algorithm in order to secure the multimedia contents before transmission and hash function algorithm in order to authenticate the received multimedia contents. The packets of multimedia contents are first encrypted using a shared public key, the same multimedia contents will also be divided into message digests through hash function algorithm to be transmitted together with the ciphertext. The receiver will then receive both the message digests and the ciphertext for the multimedia contents. The received ciphertext will be decrypted using the receiver's private key to recreate the multimedia contents. This multimedia content will then be transformed into another set of message digests by performing another hash function. The two sets of message digests (*e.g.*, received and created message digests) will be compared for authentication. When the two sets of message digests are the same, then it will be accepted and converted back to its original form of multimedia content. Otherwise, the message digests will be rejected as it can be manipulated by adversaries.

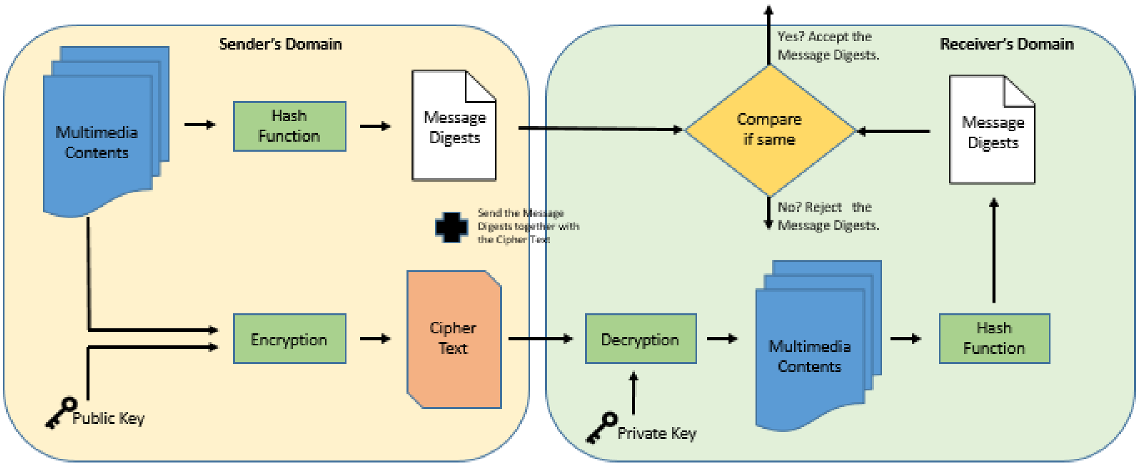


Figure 3. Design of a Secured Multimedia Contents Transmission

The integration of the asymmetric encryption and decryption algorithms provides strong security protection from possible adversary attacks while the hash function algorithm guarantees that the multimedia contents being received were not altered during the transmission. This secured multimedia contents transmission scheme can ensure that the desired multimedia contents or services by the users will be guaranteed as their integrity and authenticity have been addressed.

5. Conclusion

This paper has presented an analysis and design of a secured multimedia contents transmission scheme over the heterogeneous wireless systems. It takes full advantage of the best features of asymmetric key cryptography and hash-function algorithms to guarantee the integrity and authenticity of multimedia content or services. The proposed scheme adopts the complexity of an ECC technique for the encryption and decryption processes while the MD5 hash function algorithm was utilized to create the message digests. In the future, the scheme will be integrated with the simple symmetric key algorithms to address probable issues of confidentiality, authenticity, integrity, and non-repudiation for the transmission of multimedia contents and services.

References

[1] R. Thayer, N. Doraswamy, R. Glenn, "*IP Security Document Roadmap*", Request for Comments 2411, Internet Engineering Task Force (IETF), November 1998, https://tools.ietf.org/html/rfc2411 (accessed June 15, 2019).

[2] S. Kent, R. Atkinson, "*IP Authentication Header*", Request for Comments 2402, Internet Engineering Task Force (IETF), November 1998, https://tools.ietf.org/rfc/rfc2402.txt (accessed June 15, 2019).

[3] S. Frankel, S. Krishnan, "*IP Security (IPsec) and Internet Key Exchange (IKE) Document Roadmap*", Request for Comments 6071, Internet Engineering Task Force (IETF), February 2011, https://tools.ietf.org/html/rfc6071 (accessed June 15, 2019).

[4] S. Bellovin, "*Guidelines for Specifying the Use of IPsec Version 2*", Request for Comments 5406, Internet Engineering Task Force (IETF), February 2009, https://tools.ietf.org/html/rfc5406 (accessed June 15, 2019).

[5] D. Maughan, M. Schertler, M. Schneider, J. Turner, "*Internet Security Association and Key Management Protocol (ISAKMP)*", Request for Comments 2408, Internet Engineering Task Force (IETF), November 1998, https://tools.ietf.org/html/rfc2408 (accessed June 15, 2019).

[6] R. Barnes, M. Thomson, A. Pironti, A. Langley, "*Deprecating Secure Sockets Layer Version 3.0*", Request for Comments 7568, Internet Engineering Task Force (IETF), June 2015, https://tools.ietf.org/html/rfc7568 (accessed June 15, 2019).

[7] T. Dierks, E. Rescorla, "*The Transport Layer Security (TLS) Protocol Version 1.2*", Request for Comments 5246, Internet Engineering Task Force (IETF), (2008) August, https://tools.ietf.org/html/rfc5246 (accessed June 15, 2019).

[8] A. Freier, P. Karlton, P. Kocher, "*The Secure Sockets Layer (SSL) Protocol Version 3.0*", Request for Comments 6101, Internet Engineering Task Force (IETF), (2011) August, https://tools.ietf.org/html/rfc6101 (accessed June 15, 2019).

[9] M. Baugher, D. McGrew, M. Naslund, E. Carrara, K. Norrman, "*The Secure Real-time Transport Protocol (SRTP)*", Request for Comments 3711, Internet Engineering Task Force (IETF), (2004) March, https://tools.ietf.org/html/rfc3711 (accessed June 15, 2019).

[10] M. Bellare, P. Rogaway, "*Chapter 1: Introduction*", in Introduction to Modern Cryptography, May 11, 2005, http://web.cs.ucdavis.edu/~rogaway/classes/227/spring05/book/main.pdf (accessed June 15, 2019).

[11] W. Diffie, M. Hellman, "*New Directions in Cryptography*", IEEE Transactions on Information Theory, vol. 22, no. 6, November 1976, pp.644–654, doi: 10.1109/TIT.1976.1055638.

[12] C. Paar, J. Pelzl, "*Understanding Cryptography*", A Textbook for Students and Practitioners, Berlin: Springer-Verlag, 2010, pp.30.

[13] A. Bruen, M. A. Forcinito, "*Cryptography, Information Theory, and Error-Correction: A Handbook for the 21st Century*", John Wiley & Sons, 2011, pp.21, ISBN 978-1-118-03138-4.

[14] A. Bogdanov, D. Khovratovich, C. Rechberger, "*Biclique Cryptanalysis of the Full AES*", web.archive.org, https://web.archive.org/web/20160306104007/http://research.microsoft.com/en-us/projects/cryptanalysis/aesbc.pdf (accessed June 20, 2019).

[15] F. J. Hirsch, "*SSL/TLS Strong Encryption: An Introduction*", Apache HTTP Server, apache.org, http://httpd.apache.org/docs/2.2/ssl/ssl_intro.html#cryptographictech (accessed June 20, 2019).

[16] B. Schneier, "*Cryptanalysis of MD5 and SHA: Time for a New Standard",* schneier.com, https://www.schneier.com/essays/archives/2004/08/cryptanalysis_of_md5.html (accessed June 20, 2019).

[17] R. D. Caytiles, B. J. Park, "*ECC based Authentication Scheme for Securing Data Contents over Open Wireless Network Systems*", Journal of Advanced Information Technology and Convergence, vol. 8, no. 2, December 2018, pp.1-11, doi: 10.14801/JAITC.2018.8.2.1.