Unified 3-Tier Security Mechanism to Enhance Data Security in Mobile Wireless Networks

Zeynep Büşra KİRENCİGİL,Onurhan YILMAZ,Arif SARI

Abstract— The wide range of security mechanism proposals in wireless networks provide variety of impractical solutions for different security gaps due to the nature of the network infrastructure. Proposed mechanisms deployed in different layers classified as link, end-to-end and message segments in the proposed mechanisms stated in the literature. Security mechanisms deployed on wireless networks mainly focus on crypto algorithms for message encryption. Different mechanisms such as link encryption, message encryption and end-to-end encryption mechanisms provided to enhance data transfer security in Wireless networks. This research classifies the security mechanisms into 3 different categories for wireless networks as link, end-to-end and message encryption and proposes 3-tier mechanism by combining identification, authentication, and authorization mechanisms for each of the message, end-to-end and link encryption mechanisms. The proposed 3-tier mechanism structure is examined through OPNET simulation experiment and suggestion was made on theoretical aspect by providing new security insights.

Index Terms— *Wireless networks, Security, Simulation, 3-tier security, cryptography, enhance security mechanism*

1 Introduction

This research examined unified 3-tier security mechanism such as end-to-end, link encryption, message encryption in order to enhance data security in mobile wireless networks field. This study purposed to help to cyber security mechanisms and increase the security level by combining the well-known "identification", "authentication" and "authorization" progresses and deploy them into mobile wireless network environment to enhance data security against cyber-attacks. The latest cyber security attack proved that the country's national security is one of the main concern for public safety where.

Since the results obtained from previous researcher's related with the 3 main components. The obtained in the literature are not satisfactory about enhancing cyber security in mobile wireless networks field. This study proposes the new security mechanism in theoretical framework as unified 3-tier security mechanism by combining identification, authentication, and authorization mechanism for each of the message, end-to-end and link encryption progresses.

This article elaborates the proposed security architecture in the following sections, as the first section starts with the Data Security. In data security section symmetric cryptography, asymmetric cryptography and threshold cryptography is elaborated. The next section is explaining the proposed unified 3-tier security mechanism. It includes the end-to-end security, link encryption and message encryption steps in details. These mechanisms are combined with identification, authentication and authorization progresses. In the last part the research concludes with the proposed new security mechanism theoretically.

2. Data Security

Knowledge has become the most serious competitive weapon of the globalized business world. Every company collects variety of information developed with in the specific scope, reviews and convert new information since its first day. Once that information or resources, changes to the institutional building blocks to be always accessible and available. That simplifies our business processes in such a way that the internet, unfortunately variety of cyber-attacks, some potential risks such as internal security and virus threats brings risks with it. How to know that in the face of all these dangers and trust their information assets so important to measure it.

Data security is compulsory to ensure the continuity of the institution's work, work in a wide range of information to increase the future benefit of the reduction and investment failures can occur provides protection from threats. All information must be protected no matter what format. Nowadays, often working not only with customers, protecting information for organizations with defined business partners and shareholders, providing process control and privacy are of strategic importance.

Data security is examined under three main categories, which are are;

Privacy: To fall into the hands of unauthorized persons and to protect the information from unauthorized access.

Integrity: It is changed by unauthorized person information.

Accessibility: When the information is accessible to authorized persons is needed and available.

2.1 Cryptographic Data Security Techniques in Mobile Wireless Networks

This part examined the cryptographic data security techniques. Figure 1 shows the types of cryptographic techniques. These are Symmetric cryptography, Asymmetric cryptography, threshold cryptography and other types. In the following sections, symmetric, asymmetric and threshold cryptography are explained in details [1].

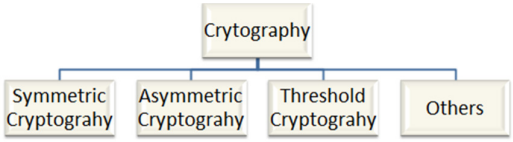

Figure1.CryptographySchema

2.1.1 Symmetric Cryptography

The encryption key is closely related to decryption key. The keys provided share the secret information between two or more parties. It is for the private communication. Large number of protocols provides various techniques. These protocols are to provide more secure but less performance. Symmetric cryptography generally used Random Nonce and Shared Key techniques.

Random nonce, in the network, a timestamp or random number (nonce) is used to make packets fresh and prevent a replay attack [2]. The session key is generally created a random number. Also in the PKI, the shared secret key can be generated from a random number, too.

Shared key: Symmetric key algorithm is the more often preferred according to asymmetric algorithms. In symmetric algorithm is less computationally intense; in implementation asymmetric algorithm slower than symmetric algorithms. The most preferred algorithms are RC4, AES, and IDEA. *"The disadvantage of shared keys in networks is that there are a total of /2 1)(−nn shared keys among n nodes in order to have a secure communication between any two nodes". "*

2.1.2 Asymmetric Cryptography

The asymmetric cryptography also known as public key cryptography. The mechanism for crypto is using two different keys for encryption and decryption. Encryption key is called as public key while decryption key is known as private key.

The public key must be sent to the receiver in advance in order to decrypt the chipper text prepared by the sender. Receiver uses private key which is generated based on the public key sent by the sender in advance to open the encrypted message. The same public key is used to reply the corresponding message by the both parties.

The public key can be visible to everyone however the decryption of the message requires generation of private key based on public key. The method-technic used to generate private key based on public key should be send to both parties since it is required for reading message content. The asymmetric encryption provides enhanced security opportunity for message contents[3].

Table1 explains the cryptographic techniques and security objectives in MANET. This table following different methods. These methods are using different techniques such as one of them is using symmetric cryptograph, another one is using threshold cryptography[4].

Table 1. Cryptographic Techniques in MANET

Scheme	Security Objectives	Techniques
ARIADNE (Hu et al, 2005)	Authentication and integrity of signal packets, based on the basic operations of DSR (Perkins, 2001).	Symmetric cryptography primitives, hash function and timestamp
ARAN, (Sanzgiri et al, 2002)	Authentication, integrity, and non-repudiation of signaling packets, based on AODV (Perkins, 2001), designed to substitute reactive routing protocols	Certificate Authority, timestamp
LEAP (Zhu et al, 2004)	Source and message one way key chain based authentication and cluster-based shared key in key management to countermeasure wormhole, sinkhole, Sybil, DoS, replay, insider attacks	Hash chain and Cluster based shared key
SEAD (Hu et al, 2005)	Authentication and integrity of signaling packets, based on DSDV (Perkins, 2001), applied to other distance vector protocols.	Hash chain and Sequence Number
SAODV (Lu et al, 2009)	Authentication and integrity of signaling packets, a security extension for AODV.	Digital signature and Hash chain
IBV (Zhang et al, 2008)	An efficient batch signature verification scheme for vehicular sensor networks.	Batch verification of ID-based signature.
SPAAR (Carter et al, 2003)	Authentication, integrity, non-repudiation, and confidentiality, secure position aided ad hoc routing protocol.	Certificate authority and timestamp.
LHAP (Zhu et al, 2003)	A hop-by-hop authentication protocol for ad-hoc networks.	Digital signature
SHELL (Younis et al, 2006)	A cluster-based key management scheme. Each cluster has its own distributed key management entity residing in a-cluster-head node. Therefore, the operational responsibility and key management responsibility are separated, which offers better resiliency against node capture.	Group shared key
SOLSR (Adjih et al, 2003)	Authentication and integrity of signaling packets	MACs and timestamp
IKM (Zhang et al, 2006)	Key management to secure mobile ad hoc network, efficient network-wide key update via a single broadcast message.	ID-based and threshold cryptography
SLSP (Papadimitratos et al, 2003)	Authentication, integrity, and non-repudiation of signal packets, extends an intrazone protocol for ZRP (Perkins, 2001).	Certificate authority

2.1.3 Threshold Cryptography

Threshold cryptography include sharing of a key by multiple seperates called shareholders engaged in encryption or decryption. The purpose is to have distributed architecture in a virulent environment. *"Other than sharing keys or working in distributed manner, TC can be*

implemented to redundantly split the message into n pieces such that with t or more pieces the original message can be recovered. This ensures secure message transmission between two nodes over n multiple paths."

Threshold schemes include key genaration, share generation, share verification, encryption and share combining algorithms. Share genaration for data integrity and confidentiality. Also it the basic requirement of threshold cryptography scheme. These schemes are being used to implement threshold variants of RSA, El Gamal, and Diffie-Hellman cryptographic algorithms that have characteristic, E (x + y) = E (x) * E (y), called homomorphism[5].

3. Proposed 3-Tier Data Security Mechanisms

Mobile security is the protection of any computing devices, and the network they connect to from threat and vulnerabilities corporate with wireless computing. Mobile security also known as wireless security. This method propose the 3-tier mechanism, it is include end-to-end security, link encryption and message encryption. End-to-end security relies on protocols and mechanisms that are implemented exclusively on the endpoints of a connection. Link encryption is an approach to communications security that encrypts and decrypts all traffic at each end of a communications line. Each tier has to make identification, authentication and authorization.

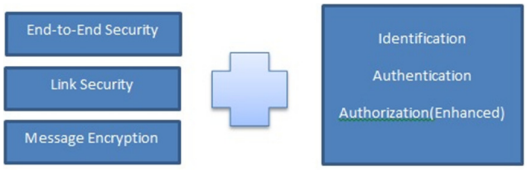

Figure 2. Proposed 3-Tier Mobile Wireless Security Mechanisms

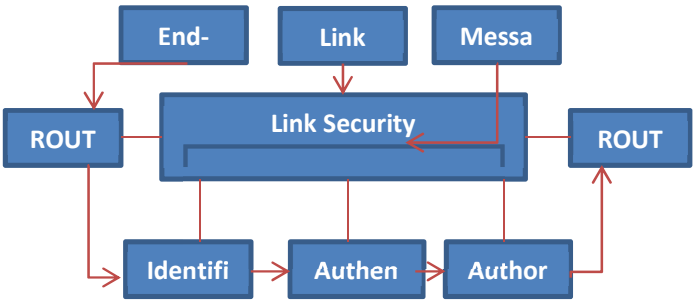

Figure 3. Proposed 3-tier security architecture

3.1. End-to-end security (hop-by-hop)

End-to-End encryption is a communication system to read only the sender and receiver of messages. Any third person or company providing the service cannot decrypt the messages transmitted. Therefore it provides data privacy and integrity.

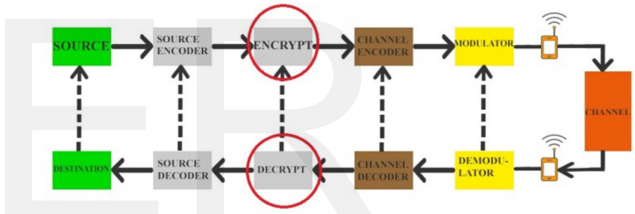

Figure 4. End-to-end encryption architecture

The network is encrypted using an encrypted algorithm called A5 to produce a 64 session key Ks. So, for every new call the necessary A5 session key Ks is created using a hash function called A8 which get the same 128 bit key Ki and 128-bit key to produce the 64 bit session key Ks. Whereas, the authentication module just works among the BS and the mobile terminal and cannot ensure hop-by-hop secure communication in the GSM network.

This research examine create a new step in the hop-by-hop security. This protocol does not apply the identification.

a)Authentication:

Datagram Transport Layer Security

All messages transferred via DTLS are prepended with 13 bytes DTLS record header. This parts define the meaning of the message, e.g. application/handshake data the version of the protocol employed, as well as a 64-bit sequence number and the record length. The high two bytes of the sequence number are used to define the period of the message which

changes once new encryption parameters have been negotiated between client and server.

The main material and cipher suite, occurring of a hash algorithm and a block cipher are negotiated between server and client before the data transferred. Handshake has a three types. First, pending an unauthenticated handshake none party authenticates with the another. Second, pending a server authenticated handshake just the server demonstrates its identity to the client. Third, in a completely authenticated handshake the client has to authenticate itself to the server as well.

4. STANDARD END-TO-END SECURITY ARCHITECTURE

This architecture is following the IoT model. Suppose that the Internet is connected by IPv6 in the close time, and component of it work 6LoWPAN. *"The transport layer in 6LoWPAN is UDP which can be considered unreliable; the routing layer is RPL or Hydro."* At the moment use Hydro for routing, because it is pretty like to RPL and it is easily available as component of the TinyOS 2.x distribution. IEEE 802.15.4 is used for the physical and MAC layer. Based on this protocol stack we chose DTLS as our security protocol. In The table 2 shown as, in the application layer on top of the UDP transport layer.

Application	CoAP, XML
Security	DTLS
Transport	UDP + IpV6 =BLIP,RPL
Network	
Medium Access/Physical	IEEE 802.15.4

Table 2. Standard End-to-End Security Architecture

Focus on the three security objectives, these are confidentiality, integrity, authenticity. For the security protocol choosing DTLS can achieve the goals. DTLS is a change of TLS for the unreliable UDP and inherits its security properties.

b)Authorization

Spanning Administrative domains

Administrative boundaries often interfere with hop-by-hop authorization. The traditional approach to authorization confuses authenticating the client to a local b administratively-defined user identity, then authorizing that user according to anaccess-control list (ACL) for the resource. *"When resources are to be shared across administrative boundaries, this scheme fails because the server has no local knowledge of the recipient's identity."*

It has many solutions for these type problems. It need to involve authenticating the remote user in local domain. It will need create account, or from the resource owner to sharing user password. "*Another approach is to install a gateway that accesses the resource with the local user's privilege but on behalf of the remote user"*. With the gateway the owner reaches user objective of sharing, however uncertain the identity and authority of the real customer from the services that supplies the underlying resources.

Spanning Protocols

Generally a gateway is installed among two systems only to translate requests by one wire protocol to other. Like any gateway, these gateways frequently inhibit the flow of authorization information by the client to server.

Spanning Levels of Abstraction

Other use for gateway programs is to present other level of separation over that ensured from a lower-level source server. Files system gets disk blocks and makes files; calendar gets record the relational database and makes event. resource code store gets the files and configuration branches. Similarly, an isolating gateway controls the lower-level source fully and only , in this way the gateway makes all access-control determinations. With hop-by-hop authorization, one can in place of authorize multiple mutually unconfidence gateways to share a single lower-level source.

Spanning Network Scales

Network measure effects an application's selection of end-to-end authorization protocol. Example of strong encryption protocol is suitable when passing a wide area network. "*Inside a*

firewall where routers are locally administered, some installations may base authority decisions on IP source addresses". On a local machine, frequently OS kernel to accurate defines the contributor in an between communication.

3.2 Link encryption

Link encryption also known as link level or link layer encryption. It is the data security process for encryption data at the link level. It is among two points within a network. Plaintext data in the host server is encrypted when it leaves the host, decrypted at the next link, then again encrypted before it runs to the next link. Every link can use a different key or different algorithm for data encryption. It is repeated until this data has achieved the receiver[6].

3.2.1 System Cipher Algorithm

The Proposed Link Encryption Algorithm (LEA) is a stream cipher algorithm. It is cryptologic concept which was improved for cipher/decipher 8-bit ASCII character. For every step, encryption or decryption, the algorithm is completed one time giving an 8-bit key character. It is associated with the plain character from bitwise extra to give the cipher character. So, there is no difference among cipher/decipher and this significant to explain just the process of encipherment. This algorithm is offering the best security level reached through the high nonlinear confuse and the finish re-initialization before each encryption process[7].

3.2.2 Intrusion Detection Systems Systems

Intrusion detection systems are generally distributed along with another protective security mechanisms, such as access control and authentication, as a second line of defense that maintains information systems. A few reasons that make intrusion detection a needed section of the entire defense system. Firstly, a few traditional system and applications were improved without security in mind. In another situation, systems and applications were improved to run in a different environment and can become undefended when distributed intrusion detection complements these protective mechanisms to develop the system security. Also, already if the protective security mechanisms can maintain information systems, it is still attractive to know what intrusions have become or becoming, than security threats and risks and so be better arranged for next attacks[8].

Snort

This network intrusion detection and prevention system excels at traffic analysis and packet logging on IP networks. Owing to protocol analysis, content searching, and diverse pre-processors, Snort detects thousands of worms, undefended exploit initiatives, port scans, and other suspect attitude. Snort uses a flexible rule-based language to define traffic that it must gather or pass, and a modular detection engine[9].

OSSEC HIDS

OSSEC HIDS makes log analysis, rootkit detection, time-based alerting, active response and integrity checking. In addition to its intrusion detection systems functionality, it is generally used as a SEM/SIM solution. Because of its strong log analysis engine, internet service protocols, data centers and universities are working OSSEC HIDS to monitor and analyze their firewalls, intrusion detection systems, authentication logs and web servers[10].

OSSIM

Its objective is to ensure a exhaustive collection of tools which, when working together, donation network/security administrators with a detailed view over each and every appearance of networks, physical access devices, servers and hosts. OSSIM associates a few other tools, including OSSEC HIDS and Nagios[11].

3.3 Message Encryption

In this section explain the message encryption methods. These methods are DES, RSA, ECC, AES. DES is a secret key encryption method. RSA, the security of a type based on the public key algorithm method. ECC is the mathematical operations of elliptic curves and elliptic curve cryptosystems based. AES is the developed by Vincent Rijmen and Joan Daemen. In the following method is DES.

3.3.1 DES

Des is secret key encryption type. The encryption process is done in block encryption. DES algorithm converts cipher text to plaintext with

64 bit key. Every encryption steps called cycle and different key is used for each cycle. DES algorithm is the special version of the Feistel encryption method. In Feistel encryption method, data encrypted to be equal two blocks in every step. Generally this two blocks descripted right block and left block.

The first process, 64 bit text to be encrypted passes to IP. Changing the locations of the bits in this encryption process takes place. First permutation change of the bits sequence is as following:

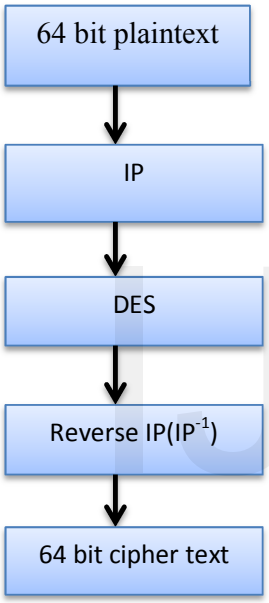

Figure 5. Encryption of 64 bit text

DES algorithm general structure

Following this step, text to be encrypted passes through the DES box. And then, 64 bits chipper text gain at the end of the opposite IP process.

DES algorithm used for a long time. Has left the palace, more advantages AES in 2000 years. But, today it is still used in areas not requiring very high security[12].

3.3.2 AES

AES developed by the Vincent Rijmen and Joan Daemen, and it was approved as a federal standard in May 2002. AES use length as 128 bits fixed block and length as 128,192 or 256 bits keys. Key differences between the number of bits in length are changing the number of AES round cycle.

$S_{0,0}$	$S_{0,1}$	$S_{0,2}$	$S_{0,3}$
$S_{1,0}$	$S_{1,1}$	$S_{1,2}$	$S_{1,3}$
$S_{2,0}$	$S_{2,1}$	$S_{2,2}$	$S_{2,3}$
$S_{3,0}$	$S_{3,1}$	$S_{3,2}$	$S_{3,3}$

Figure 6. AES Round Cycle

Figure 6 shown as, in AES algorithm method I/O and matrix is the 128 bits. Matrices are 4 lines and 4 columns. This matrix called State Matrix. In matrix are 1 byte in every segments. Every line create 32bits world.

Encryption: From text input separate 16 bytes parts and every part accommodate state matrix. All operations are possible do that, after the created state matrix. 128-bit key previously received are treated in the status matrix. State matrix of the input text is written with the first key collected.

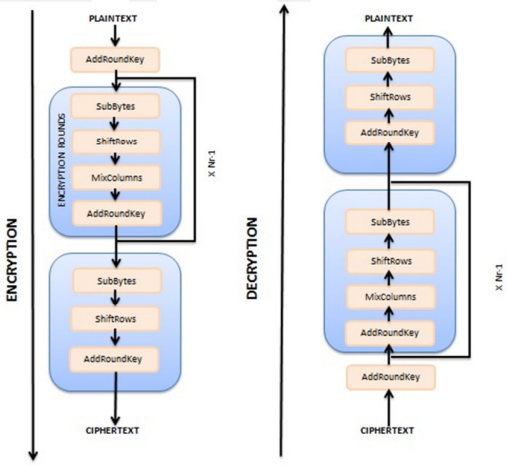

Figure 7. Encryption & Decryption of 128 bit Matrix

Each cycle can use the reverse transformation. Each cycle use 4 transformations. These are SubBytes, ShiftRows, MixColumns and

AddRoundKey. But last cycle don't use these transformations. Each cycle use different key materials. Different key materials obtain in the key planning stages. Different keys by obtain from master key and this used to for encryption.

The decryption section used reverse transformation. InvSubByte, InvShiftRows, InvMixColumns and AddRoundKey. This process reverses itself- XOR process.

AES one of the most popular symmetries algorithms, since 2010[13].

3.3.3 RSA

RSA, the security of a type based on the public key algorithm to allocate the integer to be factored in is the encryption method. RSA algorithm consists of three steps.

RSA Product Key

RSA need to a public key and a private key. A message encrypted with the public key can be solved with private key the RSA techniques. RSA keys are created as follows.

1. Selected the two different integer number. They call a and b;
2.Compute n=ab (n use mode value for private and public keys)
3. Calculate the Euler's totient function of these numbers

(a - 1)(b - 1)

4. Compute d as the multiplicative inverse of e, module (p - 1)(q - 1)
(e describes the public key)
5.P=(e;n) as the RSA public key
6.S=(d;n) as the PSA private key

RSA Encryption

Alice send to public key (n,e) to Bob, and it secret keep to private key. When Bob wants to send M message first of all M reversible with a protocol 0<m<n such that M a convert to integer. Then, compute c message such that $c=m^e \pmod n$. It can be calculated by taking the square method to quickly get to the base. Bob tranfer c to Alice.

RSA Decryption

Alice m message with a private key d encrypted messages using c is calculated as follows:
$m=c^d \pmod n$
Alice m after finding padding scheme, taking the inverse of m gets the original message[14].

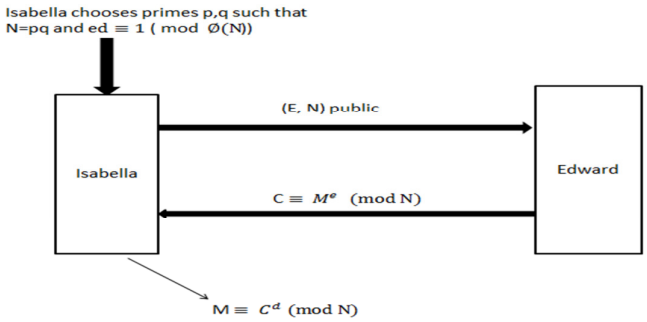

Figure 8. Encryption & Decryption progress between Isabelle & Edward

3.3.4 ECC

The benefit from the mathematical operations of elliptic curves and elliptic curve cryptosystems based. ECC crypto system called Neal Koblitz and Victor Miller has been demonstrated by in 1980[15].

Elliptic curve approach involves more mathematical procedures from the standard RSA system. the basic parts of this crypto systems (x,y) points on the eliptic curve and show the formül 1[16].

$y2 = x3 + ax + b$ with the
$x, y, a, b \in IFp = \{1, 2, 3, \ldots, p-2, p-1\}$ (1)

Encrypting the requested data is matched with the elliptic curve point in the x coordinate and create messages with their y coordinates from it against the form Qm.

More pre-shared key k value and multiplying the base point on the curve P kP coordinates are created. This multiplying value and to the required encrypting the data contained within the form of the curve on the value of Q_m collected $Q_c = Qm + kPa$ is calculated. This consists of the new point is sent to the xc counterparty of only the x coordinate. Receiver gets only Xc information from the encoding. K and P values are necessary for public key cryptography are available at himself.

Firstly calculate kP value. The data reaches the point of falling into the hands of the open state on the curve Qmin = Qc-kP is calculated in the form Qm and confidential data 'from the bit sequence is converted into data obtained by again[17].

3.3.4.TLS

TLS (Transport Layer Security) is a cryptographic protocol in Secure Sockets Layer (SSL) . The goal of the TLS is to provide data security and integrity between two communication application.TLS is protocols occur of several layers protocol. First layer is The Record Protocol and other layer is The Handshake Protocol.

In shows the figure x four clients are records protocols: TLS handshake protocol, TLS alert protocol, TLS Change Cipher Spec Protocol and application data.

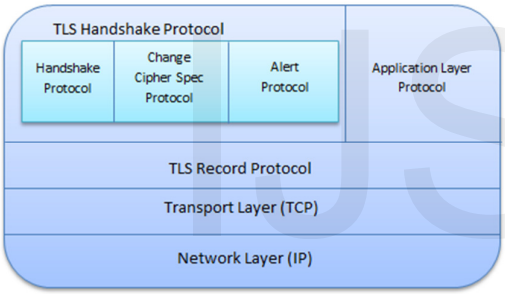

Figure.9 TLS Handshake Protocol Structure

3.3.4.1.The Record Protocol

The Record Protocol is the most bottom layer in the TLS protocol. The Record Protocol specifies an encryption and compression algorithm, and a MAC algorithm.

Compression is an optional a operation. If compression is used, received record blocks are using the same algorithm.

After compressions, data is encrypted with symmetric encryption with TLS protocol recording keys. Thus, the TLS recording protocol provides e confidentiality and integrity services. Different symmetric encryption key is used for each connection. There are four types of MACs. Unconditionally secure each the cipher text of the message authenticates itself, as nobody doesn't access.

Hash function-based MACs, in which key are used in together with a hash function stream cipher-based. Stream cipher based, in which secure stream cipher is used to separate a message into two sub-streams and each sub-stream is fed into a LFSR. Block cipher-based, in which message blocks are encrypted using block cipher.

Decoding is the reverse of encoding operation and uses the same secret key.

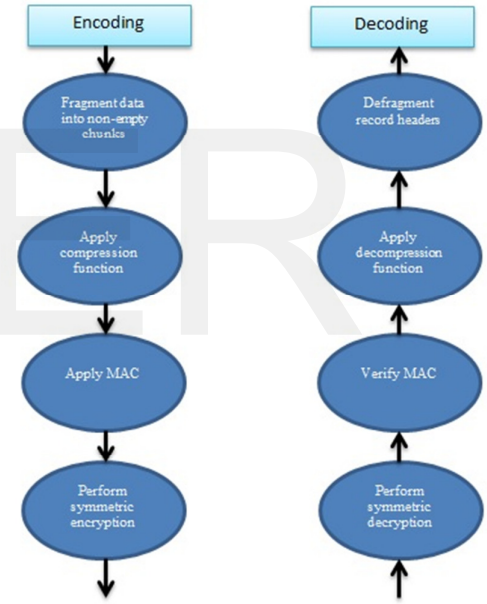

Figure 10. Encoding And Decoding Of Data In Record Layer

3.3.4.2.The Handshake Protocol

The Handshake Protocol is highest-layer in TLS protocol. TLS handshake protocol to communicate with the other parties' authorization, the mutual exchange of encryption algorithm and key provided. Two kinds of handshake are full handshake and abbreviated handshake.

Full handshake: The TLS handshake protocol corporate handshake with series of steps. When handshake steps start secure connection client is request and end when the secure connection among two peers is establish. All steps finished in the full handshake protocol.

Abbreviated handshake: *An abbreviated handshake can be used if a secure connection was previously established. The peers cache a previous session and use the same security parameters of this session when this session is requested to be resumed.*

Conclusion

This research paper exposed the requirements of lightweight security algorithm for mobile wireless networks through implementation of Unified 3-Tier Security Mechanism to Enhance Data Security in Mobile Wireless Networks by combining link layer, message encryption as well as point to point security.
The proposed combinations of algorithms are required to be deployed in wireless networks to enhance organizational data security within organizational wireless networks. The main aim is to enhance security by taking into consideration of nature of wireless networks where majority of the proposed algorithms and architectures cannot be deployed on them. The further researchers can be conducted on the basis of lightweight intrusion detection and mitigation systems for wireless networks by taking into consideration of both message encryption, link encryption and end-to-end encryption for better and enhanced security.

References

[1]Jianmin Chen and Jie Wu , A Survey on Cryptography Applied to Secure Mobile Ad Hoc Networks and Wireless Sensor Networks

[2] Network Security: Private Communication in a Public World,Kaufman, Perlman, & Speciner, 2002.

[3]Dr. Atul M. Gonsai1 , Lakshadeep M. Raval2, International Journal of Computer Trends and Technology (IJCTT) – volume 11 number 1 – May 2014, Evaluation of Common Encryption Algorithm and Scope of Advanced Algorithm for Simulated Wireless Network Available at: http://www.ijcttjournal.org/Volume11/number-1/IJCTT-V11P102.pdf)

[4] A Survey on Cryptography Applied to Secure Mobile Ad Hoc Networks and Wireless Sensor Networks, Jianmin Chen and Jie Wu,Available at: http://www.cse.fau.edu/~jie/research/publications/Publication_files/wsn-chapter-111%5B1%5D.pdf

[5] Security of Ad Hoc Networks and Threshold Cryptography Levent Ertaul, Nitu Chavan California State University, Hayward

[6] A Graduate Course in Applied Cryptography, Dan Boneh, Victor Shoup.

[7] 1st National Radio Science Conference (NRSC2014) April 28 – 30, 2014, Faculty of Engineering, Ain Shams University, Egypt, C2. Design of LEA: Link Encryption Algorithm, NEW PROPOSED STREAM CIPHER Algorithm by Hadia M. El Hennawy , Alaa E. Omar , Salah M. Kholaif.

[8] Volume 2, Issue 8, August 2012 ISSN: 2277 128X International Journal of Advanced Research in Computer Science and Software Engineering, Research Paper Available online at: www.ijarcsse.com An Overview on Intrusion Detection System and Types of Attacks It Can Detect Considering Different Protocols

[9] Proceedings of LISA '99: 13th Systems Administration Conference,Seattle, Washington, USA, November 7–12, 1999SNORT—LIGHTWEIGHT INTRUSION DETECTION FOR NETWORKS ,Martin Roesch

[10] Intrusion Detection using Open Source Tools,Jack TIMOFTE

[11] OSSEC&OSSIM Unified Open Source Securirty Mechanism. OSSEC Company.

[12] ITU, DES BLOK ŞİFRELEME ALGORİTMASININFPGA ÜZERİNDE DÜŞÜK ENERJİLİ TASARIMI,Tarık KAPLAN

[13] Federal Information Processing Standards Publication 197 November 26, 2001 Announcing the ADVANCED ENCRYPTION STANDARD (AES)

[14] The Mathematics of the RSA Public-Key Cryptosystem,Burt Kaliski ,RSA Laboratories

[15] A Dissertation Submitted to the ,Graduate School in Partial Fulfillment of the Requirements for the Degree of MASTER of SCIENCE ,Department: Computer Engineering ,Major: Computer Software ,Izmir Institute of Technology ,Izmir, Turkey

[16] Digital Signature Application work with ECC, Tarık YERLİKAYA,Ercan BULUŞ Derya ARDA
[17] ENHANCING SECURITY FOR MOBILE AD HOC NETWORKS,BY USING ELLIPTIC CURVE CRYPTOGRAPHY ,Rubaiyat Islam Rafat [MIT-806],Md. Majharul Haque [MIT-815]