Proposal for SZRP Protocol with the Establishment of the Salted SHA-256 Bit HMAC PBKDF2 Advance Security System in a MANET

Md.Torikur Rahman
Institute Of Information Technology
Jahangirnagar University
Dhaka, Savar-1342
Email:torikurrahman@gmail.com

Md.Julkar Nayeen Mahi
Institute Of Information Technology
Jahangirnagar University
Dhaka, Savar-1342
Email: mahi.1992@gmail.com

***Abstract*—The cooperative junction of mobile nodes consists of any centralized access point or a self-configuring network existing infrastructure without the required intervention is called ad hoc network. A well designed security protocol is a challenging task due to its unique characteristics such as, lack of central authority, frequent topology changes, rapid node mobility, shared radio channel and limited availability of resources for ad hoc network. However, most of these protocols are two kinds. They are proactive and reactive in terms. Both of these approaches contains their own limitations, for example, in maintaining the routing information the proactive protocols use excess bandwidth while, the reactive ones have long route request delay. In this paper, we proposed a secure hybrid ad hoc routing protocol, called Secure Zone Routing Protocol (SZRP). The proposed protocol is based on the concept of zone routing protocol (ZRP) with AES (Advanced Encryption System).**

Key terms- IARP, IERP, Hashing, SHA-256bit, HMAC, PBKDF2.

I. Introduction

Mobility is becoming rapidly important for users of computing systems. Technology has made distance smaller, less expensive and more powerful with wireless communicating devices and computers. The necessary mobile computing support is being provided in some areas by installing base stations and access points. Mobile users can maintain their connectivity by accessing this infrastructure from home, office, or while on the road. If mobile users want to communicate in the absence of a support structure, they must form an ad hoc network.

A mobile ad hoc network (MANET) is a wireless network, comprised of mobile computing devices (nodes) that use wireless transmission for communication, without the help of any established infrastructure or centralized administration such as a base station in cellular network or an access point in wireless local area network [1]. Figure 1 shows an example of mobile ad hoc network and its communication technology.

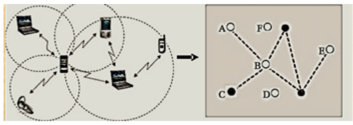

Fig. 1: A Typical Mobile Ad Hoc Network

II. Routing approaches in mobile ad hoc network

There are generally categorized as table-driven or proactive, on-demand or reactive and hybrid routing protocols in Fig 2.

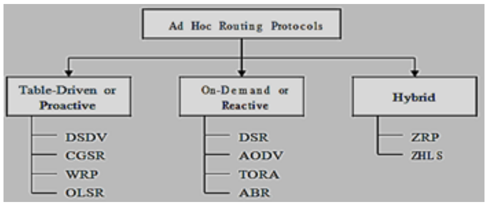

Fig. 2: Classifications of Ad Hoc Routing Protocols

III. Zone routing protocol(ZRP)

In a MANET, it is either a purely proactive or purely reactive approach to implement a routing protocol for it, but it has some disadvantages. The Zone Routing Protocol (ZRP) as described in [5] aims at addressing these limitations by combining the best characteristics of both proactive and reactive approaches and hence it can be classed as a hybrid proactive/reactive routing protocol. Most communication takes place between nodes close to each other. ZRP reduces the proactive scope to a zone centered on each node and reactive approach outside the zone. When a node has a data packet for a particular destination, it checks whether the destination is within its zone or not. If it is within the zone, the packet is routed proactively. Reactive routing is used if the destination is outside the zone.

A. Routing

A node that has a packet to send first checks whether the destination is within its local zone or not using information provided by IARP routing table[10]. If the destination is within the zone, then the IARP routing table must have a valid route to the destination. So in this case, the packet is routed proactively to the intra-zone destination. Reactive routing is used if the destination is outside the zone[12]. The reactive routing process is divided into two phases: the route request phase and the route reply phase.

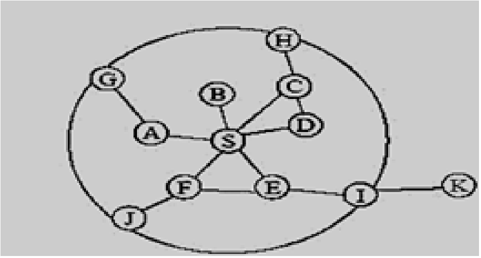

Fig. 3: Routing zone of node S with zone radius =2 (is the number of hops of the zone)

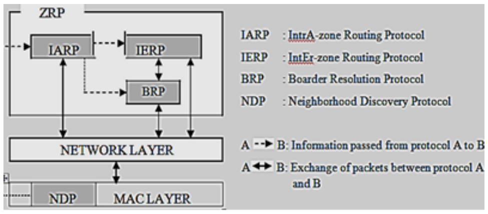
ZRP
IARP
IERP
BRP
NETWORK LAYER
NDP
MAC LAYER
IARP : IntrA-zone Routing Protocol
IERP : IntEr-zone Routing Protocol
BRP : Boarder Resolution Protocol
NDP : Neighborhood Discovery Protocol
A B: Information passed from protocol A to B
A B: Exchange of packets between protocol A and B

Fig. 4: ZRP Architecture

IV. Protocol overview of the secure zone routing protocol(SZRP))

Neither a pure proactive nor a pure reactive approach provides a full solution for secure ad hoc routing that performs efficiency across a wide range of operational requisites and network configuration. For a complete, efficient and implementable solution for secure routing is highly desirable that can operate well on diverse applications of ad hoc networks. In our proposal we use hash function in an MANET.

The Secure Zone Routing Protocol (SZRP) is developed on the concept of Zone Routing Protocol (ZRP) [3, 4]. It is a hybrid routing protocol that is comprised of the best features of both proactive and reactive approaches and adds its own security mechanisms to perform secure routing. The reasons for selecting ZRP as the basis of our protocol are as follows:

ZRP is based on the concept of routing zones, a restricted area, and it is more feasible to apply the security mechanisms within a restricted area than in a broader area that of the whole network[11]. Since the concept of zones separate the communicating nodes in terms of interior (nodes within the zone) and exterior (nodes outside the zone) nodes, certain information like network topology and neighborhood information etc. can be hidden to the exterior nodes, In case of a failure, it can be restricted to a zone.

Like ZRP the proposed protocol performs routing in terms of intra-zone [5] and inter-zone [5] routing. However, it differs from ZRP in security aspects. In ZRP where there is no security consideration, SZRP is designed to address all measure security concerns like end to end authentication, message/packet integrity and data confidentiality during both intra and inter-zone routing.

A. Architecture

The architectural design of SZRP is shown in Figure: 5 the proposed architecture is a modification of ZRP [3].

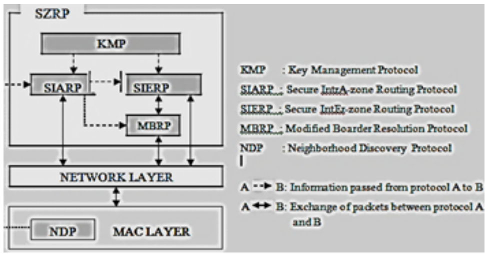
SZRP
KMP
SIARP
SIERP
MBRP
NETWORK LAYER
NDP
MAC LAYER
KMP : Key Management Protocol
SIARP : Secure IntrA-zone Routing Protocol
SIERP : Secure IntEr-zone Routing Protocol
MBRP : Modified Boarder Resolution Protocol
NDP : Neighborhood Discovery Protocol
A B: Information passed from protocol A to B
A B: Exchange of packets between protocol A and B

Fig. 5: SZRP Architecture

TABLE I: Table of notations

Notation	Description
SKx	Signature Key of node X
VKx	Signature verification key for node X
EKx	Encryption Key for node X
DKx	Decryption Key of node X
[d] SKx	Packet d signed with SKx, this can be only verified using VKx
[d]EKx	Message d encrypted with EKx, this can be only decrypted with DKx
[d]—b	b is appended to the packet containing d
CERTx	Public key certificate of X
IPx	IP address of X
T	Time stamp
E	Certificate expiration time
Nx	Nonce issued by node X
SKREQ	Session Key Request packet identifier
SKREP	Session Key Reply packet identifier
SRD	Secure Route Discovery packet identifier
SRR	Secure Route Reply packet identifier
ERR	Error packet identifier

B. The secure routing algorithm

This section describes the secure intra-zone and inter-zone routing in details. We consider the network in Figure 6 for the illustration.

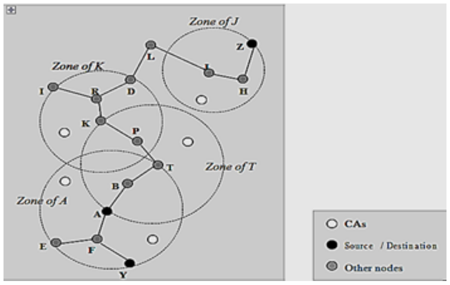

Fig. 6: Intra-zone and Inter-zone destinations of node A (zone radius = 2)

C. Secure intra-Zone routing (IARP)

The Intra zone Routing Protocol (IARP) [5] is a limited scope proactive routing protocol, which is used to support a primary global routing protocol. The routing zone radius shows the scope of the proactive part, the distance in hops that IARP route updates relayed. IARP's proactive tracking of local network connectivity provides support for route acquiring and route maintenance. First routes to local nodes are immediately available, avoiding the traffic overhead and latency of a route discovery.Here is the intra-zone routing activity overview of our network.

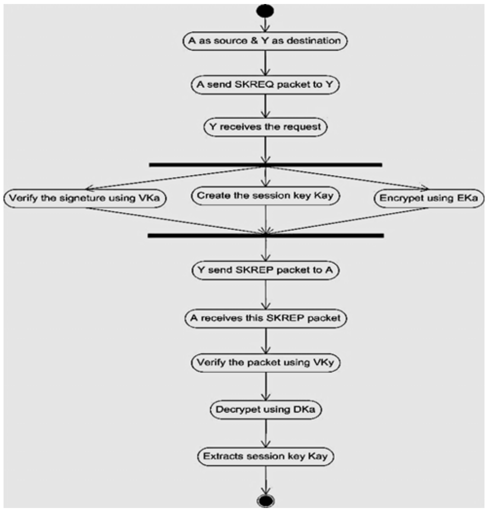
A as source & Y as destination
A send SKREQ packet to Y
Y receives the request
Verify the signeture using VKa
Create the session key Kay
Encrypet using EKa
Y send SKREP packet to A
A receives this SKREP packet
Verify the packet using VKy
Decrypet using DKa
Extracts session key Kay

Fig. 7: Basic activity diagram of Secure Intra-zone routing

D. Secure inter-Zone routing (IERP)

The Inter-zone Routing Protocol (IERP) is the global reactive routing component of the Zone Routing Protocol (ZRP) [3].IERP adapts existing reactive routing protocol implementations to take advantage of the known topology of each nodes surrounding R-hop neighborhood (routing zone), provided by the Inter-zone outing Protocol (IARP)[5]. The availability of routing zone routes allows IERP to suppress route queries for local destinations.Here is the inter-zone routing activity overview of our network.

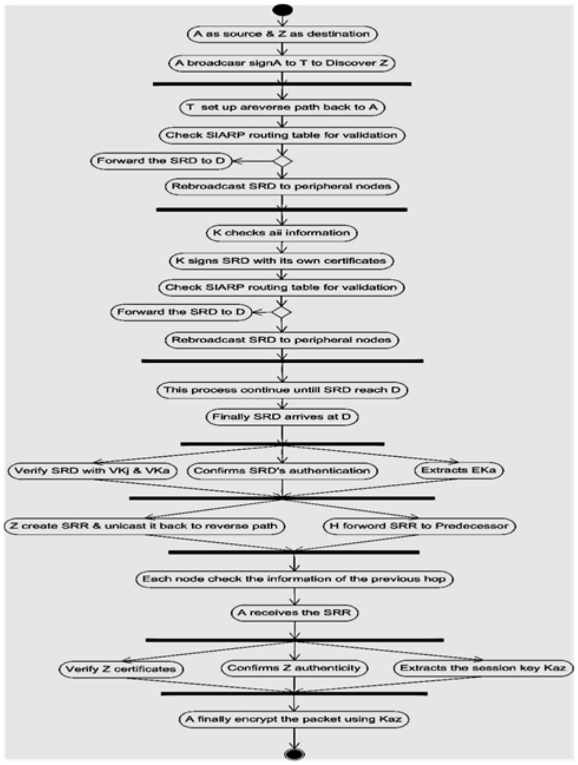
A as source & Z as destination
A broadcasr signA to T to Discover Z
T set up areverse path back to A
Check SIARP routing table for validation
Forward the SRD to D
Rebroadcast SRD to peripheral nodes
K checks aii information
K signs SRD with its own certificates
Check SIARP routing table for validation
Forward the SRD to D
Rebroadcast SRD to peripheral nodes
This process continue untill SRD reach D
Finally SRD arrives at D
Verify SRD with VKj & VKa
Confirms SRD's authentication
Extracts EKa
Z create SRR & unicast it back to reverse path
H forword SRR to Predecessor
Each node check the information of the previous hop
A receives the SRR
Verify Z certificates
Confirms Z authenticity
Extracts the session key Kaz
A finally encrypt the packet using Kaz

Fig. 8: Basic activity diagram of Secure Inter-zone routing

V. Message encryption

Message encryption is the technique of transforming a message into a disguised message which no unauthenticated individual can read, but which can be restored in its genuine form by an intended receiver. The plaintext is converted into cipher text by the process of encryption, which can be done by the use of certain algorithms or functions[17]. The reverse process is termed as decryption [7]. The process of encryption and decryption are governed by keys, which are small amount of information used by the cryptographic algorithms. Asymmetric key algorithm is comparatively slower process than symmetric but could be a great use in the establishment of a secure network system[20].Here we use the asymmetric-key cryptography for our proposed network.

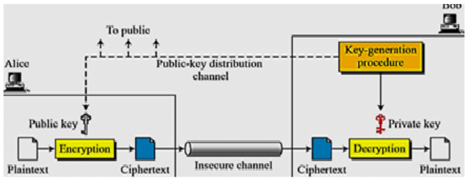

Fig. 9: Public key cryptography (Asymmetric-key)

VI. Password hashing

Hash algorithms are one way functions turn any amount of data into a fixed-length ”fingerprint” that cannot be reversed. This is great for protecting passwords, because we want to store passwords in an encrypted form that’s impossible to decrypt, but at the same time, we need to be able to verify that a user’s password is correct. The general workflow for account registration and authentication in a hash-based account is as follows-

hash(”hello”)=2cf24dba5fb0a30e26e83b2ac5b9e29e1b161e hash(”hbllo”)=58756879c05c68dfac9866712fad6a93f8146f

Only cryptographic hash functions may be used to implement password hashing like SHA256, SHA512, RipeMD, and WHIRLPOOL. Here we use SHA-256 digest message authentication for the security.

A. Salt password hashing

The best way to protect passwords is to employ salted password hashing. The process below will explain how to do it properly.

hash(”hello”)=2cf24dba5fb0a30e26e83b2ac5b9e29e hash(”hello”+”QxLU”)=9e209040c863f84a31e719795b257752 (salted)

We can prevent above described attacks by randomizing each hash, so that when the same password is hashed twice, the hashes are not the same. We can randomize the hashes by appending or prepending a random string, called a salt, to the password before hashing. As shown in the example above, this makes the same password hash into a completely different string every time. To check if a password is correct, we need the salt, so it is usually stored in the user account database along with the hash.

B. SHA

SHA stands for Secure Hash Algorithm and its a family of cryptographic hash functions[23]. Weve created a user login page as an example for a zone network system to encrypt the password and also you can see how to decrypt it for security purpose[26].

C. Keyed Hashes and Password Hashing Hardware with advance functions

We think that to add a secret key to the hash so that only someone who knows the key can use the hash to validate a password. This can be accomplished with two ways. Either the hash can be encrypted using a cipher like AES[22], or the secret key can be included in the hash using a keyed hash algorithm like HMAC. We consider it necessary for any service hosting more than 1,000,000 user accounts.

VII. Why do we have to use a special algorithm like HMAC ? Why can't we just append the password to the secret key ?

Hash functions like MD5, SHA1, and SHA2 use the MerkleDamgrd construction, which makes them vulnerable to what are known as length extension attacks[21]. This means that given a hash H(X), an attacker can find the value of H(pad(X) + Y), for any other string Y, without knowing X. pad(X) is the padding function used by the hash. This means that given a hash H (key + message), an attacker can compute H(pad(key + message) + extension), without knowing the key. If the hash was being used as a MAC, then by using the key we can prevent an attacker from being able to modify the message and replace it with a different valid hash, in case of that the system has failed, since the attacker now has a valid hash of message + extension. A clever cryptographer may one day come up with a clever way to use these attacks to make cracking faster, so in case of that we must use HMAC.

VIII. PBKDF2 and its workflow

The Public-Key Cryptography Standards (PKCS) 5 [RFC2898] has discovered a function that is Password-Based Key Derivation Function 1. PBKDF2 is the second generation or advanced system security function of PBKDF1; can be described in short form as (PBKDF2) is used by several protocols to derive encryption keys from a password[18].

For example, Salted Challenge Response Authentication Mechanism (SCRAM) [RFC5802] uses PBKDF2 with Hash-based Message Authentication Code (HMAC) [RFC2104] and Secure Hash Algorithm (SHA).

A. PBKDF2,HMAC and SHA2 test vectors

The input strings below are encoded using ASCII [ANSI.X3-4.1986].The sequence (without quotation marks) means a literal ASCII NULL value (1 octet). "DK" refers to the Derived Key.

Input: P = "password" (8 octets) S = "salt" (4 octets) c = 16777216 dkLen = 20

Output: DK = eefe 3d 61 cd 4d a4 e4 e9 94 5b 3d 6b a2 15 8c 26 34 e9 84 (20 octets)

Input: P = "passwordPASSWORDpassword" (24 octets) S="saltSALTsaltSALTsaltSALTsaltSALTsalt" (36 octets) c = 4096 dkLen = 25

Output: DK = 3d 2e ec 4f e4 1c 84 9b 80 c8 d8 36 62 c0 e4 4a 8b 29 1a 96 4c f2 f0 70 38 (25 octets)

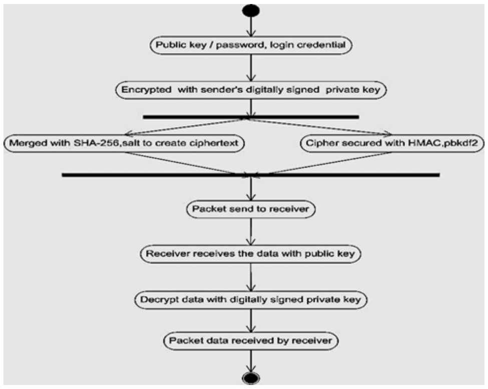
Public key / password, login credential
Encrypted with sender's digitally signed private key
Merged with SHA-256,salt to create ciphertext
Cipher secured with HMAC,pbkdf2
Packet send to receiver
Receiver receives the data with public key
Decrypt data with digitally signed private key
Packet data received by receiver

Fig. 10: Asymmetric-key , SHA-256 bit HMAC and PBKDF2 security system.

IX. Overview of our network

Here we are thinking to use cryptography to secure our network between two zones. In here,if we think two network zones as two locations with in an area, then it will be a clear view to all. In the picture below we see that two locations are using one protocol, that is (ZRP). From library room to presentation room are connected with two server using bridge protocol. The two server are using cryptography algorithms SHA-256 bit,HMAC and PBKDF2 functions for authentication.First zone1 sends requests to zone2.In this case zone1 uses a public key for the network to connect with zone2, zone2 also uses the same method. For sending data first zone1 encrypts the message using own private key and sends its cipher message through the public key that is using in the network.Then the cipher message is decrypted by zone2 using its own private key. By using own network public key we ensure a secured channel over the network.If zone2 replies to zone1 ,then it also does the same.

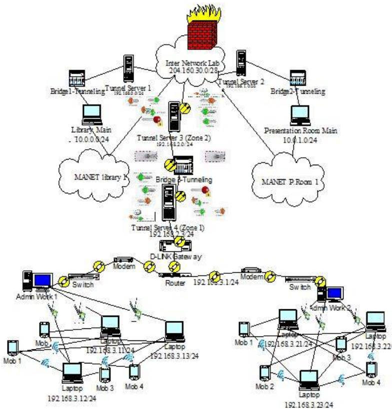

Fig. 11: Overview of our network

X. Conclusion

In this paper, we have explored the advantages of hybrid routing in dealing with these limitations, where the proactive and the reactive behavior is mixed in the amounts that best match these operational conditions. We have presented the design and analysis of a new secure routing protocol for mobile ad hoc networks, called the SZRP. The secured version of ZRP. The proposed protocol gives a better solution towards achieving the security goals like message integrity, data confidentiality and message authentication, by taking an integrated approach of digital signature and asymmetric key encryption and decryption techniques with the help of SHA-256, HMAC and pbkdf2 advance security system. Yet slower process, but ensures greater security administrative privileges.

References

[1] Perkins and Charles E, *A Guide to Adhoc networking*. Harlow, England: Addison-Wesley, 2008.

[2] E.M. Belding-Royer and C. K. Toh, *A review of current routing protocols for ad-hoc mobile wireless networks*. IEEE Personal Communications Magazine, 1999.

[3] Haas Z. J., Pearlman M. R., and Samar P., *The Zone Routing Protocol (ZRP)*. IETF Internet Draft, draft-ietf-manet-zone-zrp-04.txt, July 2002.

[4] Jan Schaumann, *Analysis of Zone Routing Protocol*. Stevens Institute of Technology Hoboken, New Jersey, USA, 8th December 2002.

[5] Haas, Zygmunt J., Pearlman, Marc R., Samar, *Intrazone Routing Protocol (IARP)*. IETF Internet Draft, draft-ietf-manet-iarp-01.txt, June 2001.

[6] Devi, BAS Roopa and Murthy, JVR and Narasimha, *Secure zone based routing protocol for mobile adhoc networks*. IEEE,2013.

[7] K.Sanzgir, and B.Dahill, *A secure routing protocol for ad hoc networks*. Proceeding of the 10th IEEE International Conference on Network Protocols, 2002.

[8] Behrouz A. Forouzan, *Cryptography and Network Security*. Special Indian Edition, Tata McHill publication, 2007.

[9] Mohapatra, Prasant and Krishnamurthy, Srikanth, *AD HOC NETWORKS: technologies and protocols*. Springer,2005.

[10] Boukerche, Azzedine, *Algorithms and protocols for wireless, mobile Ad Hoc networks*. John Wiley and Sons, 2008.

[11] Sarkar, Subir Kumar and Basavaraju, TG and Puttamadappa, *Ad hoc mobile wireless networks: principles, protocols and applications*. CRC Press, 2007.

[12] Hekmat, Ramin, *Ad-hoc Networks: Fundamental Properties and Network Topologies*. Springer,2006.

[13] Barbeau, Michel and Kranakis, Evangelos, *Principles of Ad-hoc Networking*. John Wiley and Sons,2007.

[14] Pathan, Al-Sakib Khan, *Security of self-organizing networks: MANET, WSN, WMN, VANET*. CRC press,2010.

[15] Kaufman, Charlie and Perlman, Radia and Speciner, Mike, *Network security: private communication in a public world*. Prentice Hall Press,2002.

[16] Falk, Matthew D, *Cryptographic cloud storage framework*. Massachusetts Institute of Technology,2013.

[17] Viega, John and Messier, Matt, *Secure Programming Cookbook for C and C++: Recipes for Cryptography, Authentication, Input Validation and More*. O'Reilly Media, Inc.,2003.

[18] Josefsson, Simon, *PKCS# 5: Password-Based Key Derivation Function 2 (PBKDF2) Test Vectors*. 2011.

[19] Cheddad, Abbas and Condell, Joan and Curran, Kevin and McKevitt, Paul, *A hash-based image encryption algorithm*. Elsevier, 2010.

[20] Orman, Hilarie and Hoffman, Paul, *Determining strengths for public keys used for exchanging symmetric keys*. 2004.

[21] William, E Burr, *Selecting the advanced encryption standard*. IEEE Security and Privacy, IEEE Computer Society,2003.

[22] Lee, Jesang and Chang, Donghoon and Kim, Hyun and Lee, Eunjin and Hong, Deukjo and Sung, Jaechul and Hong, Seokhie and Lee, Sangjin, *A New 256-bit Hash Function DHA-256: Enhancing the security of SHA-256*. 2005.

[23] Gilbert, Henri and Handschuh, Helena, *Security analysis of SHA-256 and sisters*. Springer,2004.

[24] Hirose, Shoichi and Ideguchi, Kota and Kuwakado, Hidenori and Owada, Toru and Preneel, Bart and Yoshida, Hirotaka, *A lightweight 256-bit hash function for hardware and low-end devices*. Springer,2011.

[25] Goldwasser, Shafi and Micali, Silvio and Rivest, Ronald L, *A digital signature scheme secure against adaptive chosen-message attacks*. SIAM,1988.

[26] Cheddad, Abbas and Condell, Joan and Curran, Kevin and McKevitt, Paul, *A hash-based image encryption algorithm*. Elsevier,2010.