ISSN- 2350-0530(O), ISSN- 2394-3629(P)
IF: 4.321 (CosmosImpactFactor), 2.532 (I2OR)
InfoBase Index IBI Factor 3.86

INTERNATIONAL JOURNAL OF RESEARCH – GRANTHAALAYAH
A knowledge Repository

Science

SECURE ROUTING IN MANET USING HYBRID CRYPTOGRAPHY

D.Sivamurugan [*1], L.Raja [2]
[*1]PG Student, ECE, K.S.R College of Engineering, Tamilnadu, India
[2]Associate Professor, ECE, K.S.R College of Engineering, Tamilnadu, India

DOI: https://doi.org/10.29121/granthaalayah.v5.i4.2017.1798

Abstract

Mobile ad hoc network (MANET) is a group of mobile nodes that communicates with each other without any supporting infrastructure. These networks have some unique features such as dynamic mobility, open nature, lack of infrastructure, limited physical security and they are vulnerable to several security threats. Malicious node can drop all or partial received packets instead of forwarding them to the next hop through the path. In order to find the malicious nodes, an initial transmission is made between the source and destination nodes. Using fuzzy rules, the trust value of each node is computed and it varies from 0 to 1. A common threshold value is set for each node and by using this threshold value, every node in the network can be identified as either a malicious node or a regular node. After identifying the malicious nodes, these nodes are eliminated by muting the power to off state. As the malicious nodes are eliminated between source and destination nodes, source node can select another trusted path to its destination node. For security and authentication of routing information, hybrid cryptography is employed, using advanced encryption standard (AES) and elliptic curve cryptography (ECC) algorithms. AES algorithm is used as symmetric algorithm to encrypt the routing information and ECC algorithm is used as asymmetric algorithm to encrypt the public key. During encryption, the original plain text is converted into cipher text with encrypted public key and similarly during decryption cipher text is converted into original plain text with decrypted private keys. So the proposed method involves both AES and ECC algorithms which provides security mechanism as efficient and sufficient one. The experimental simulations are carried for the proposed model using network simulator 2 (NS-2) for Throughput, Delay, Packet delivery ratio, Packet overhead and Packet drop.

Keywords: Advanced Encryption Standard (AES); Elliptic Curve Cryptography (ECC); Network Simulator (Ns-2); Mobile Ad Hoc Network (MANET); Trust Value (TV).

Cite This Article: D.Sivamurugan, and L.Raja. (2017). "SECURE ROUTING IN MANET USING HYBRID CRYPTOGRAPHY." *International Journal of Research - Granthaalayah*, 5(4), 83-91. https://doi.org/10.29121/granthaalayah.v5.i4.2017.1798.

ISSN- 2350-0530(O), ISSN- 2394-3629(P)
IF: 4.321 (CosmosImpactFactor), 2.532 (I2OR)
InfoBase Index IBI Factor 3.86

1. Introduction

Mobile Ad-hoc network is a set of wireless devices called wireless nodes, which dynamically connect and transfer information. Wireless nodes can be personal computers (desktops/laptops) with wireless LAN cards, Personal Digital Assistants (PDA), or other types of wireless or mobile communication devices. In general, a wireless node can be any computing equipment that employs the air as the transmission medium. The wireless node may be physically attached to a person, a vehicle, or an airplane, to enable wireless communication among them.

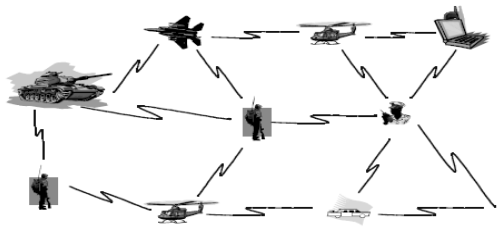


Figure 1: Overview of Mobile Ad-hoc Network

In MANET, a wireless node can be the source, the destination, or an intermediate node of data transmission. When a wireless node plays the role of intermediate node, it serves as a router that can receive and forward data packets to its neighbor closer to the destination node. Due to the nature of an ad-hoc network, wireless nodes tend to keep moving rather than stay still. Therefore the network topology changes from time to time.

2. Current Challenges

In a mobile ad hoc network, all the nodes cooperate with each other to forward the packets in the network, and hence each node is effectively a router. Thus one of the most important issues is routing. This focuses mainly on routing issues in ad hoc networks. In this section, some of the other issues in ad hoc networks are described:

Distributed Network
A MANET is a distributed wireless network without any fixed infrastructure. That means no centralized server is required to maintain the state of the clients.

Dynamic Topology
The nodes are mobile and hence the network is self-organizing. Because of this, the topology of the network keeps changing over time. Consequently, the routing protocols designed for such networks must also be adaptive to the topology changes.

Power Awareness
Since the nodes in an ad hoc network typically run on batteries and are deployed in hostile terrains, they have stringent power requirements. This implies that the underlying protocols must be designed to conserve battery life.

ISSN- 2350-0530(O), ISSN- 2394-3629(P)
IF: 4.321 (CosmosImpactFactor), 2.532 (I2OR)
InfoBase Index IBI Factor 3.86

Addressing Scheme

The network topology keeps changing dynamically and hence the addressing scheme used is quite significant. A dynamic network topology requires a ubiquitous addressing scheme, which avoids any duplicate addresses. In wireless WAN environments, Mobile IP is being used. Because the static home agents and foreign agents are needed, hence, this solution is not suitable for ad hoc network.

Network Size

The ability to enable commercial applications such as voice transmission in conference halls, meetings, etc., it is an attractive feature of ad hoc networks. However, the delay involved in the underlying protocols places a strict upper bound on the size of the network.

Security

Security in an ad hoc network is extremely important in scenarios such as a battlefield. The five goals of security – availability, confidentiality, integrity authenticity and non-repudiation - are difficult to achieve in MANET, mainly because every node in the network participates equally in routing packets.

3. Related Work

An Energy Efficient Routing Algorithm for Mobile Ad Hoc Networks, Horst F. Wedde, Muddassar Farooq, Thorsten Pannenbaecker, Bjoern Vogel, Christian Mueller, Johnannes Meth and Rene Jeruschkat (June 2005) [5] presented a new routing algorithm for energy efficient routing in mobile ad hoc networks. The algorithm is inspired by the foraging principles of honey bees. The algorithm mainly utilizes two types of agents, scouts and foragers, for doing routing in mobile ad hoc networks. BeeAdHoc is a reactive source routing algorithm and it consumes less energy as compared to existing state-of-theart routing algorithms because it utilizes less control packets to do routing. The results of extensive simulation experiments show that BeeAdHoc consumes significantly less energy as compared to DSR, AODV and DSDV which are state-of-the-art routing algorithms, without making any compromise on traditional performance metrics (packet delivery ratio, delay and throughput).

[3], AES-ECC Encryption System based on FPGA in WSNs, Bing Ji, Liejun Wang and Qinghua Yang (2015) tells that according to the threat of the data transmission on wireless sensor networks, a technique for speeding up point multiplication, an improved AES-ECC hybrid encryption system with cross encrypted keys for secure key exchange is presented. This scheme use AES algorithm to encrypt data, use ECC algorithm to encrypt private key and use SHA-1 algorithm and ECC algorithm to generate digital signature. With rapid advances in VLSI technology, a highly parallel FPGA design is used for their scheme, the computing efficiency of the algorithm is greatly improved. The AES encryption module and multi-scalar multiplication algorithm is also optimized. [10], AES and ECC Mixed for ZigBee Saif Al-alak, Zuriati Ahmed, Azizol Abdullah and shamala subramiam (2011) proposed the security protocols of ZigBee wireless sensor network in MAC layer. AES 128-bit encryption algorithm in CCM* mode is secure transferred data; however, AES's secret key will be break within nearest future. Efficient public key algorithm, ECC has been mixed with AES to rescue the ZigBee wireless sensor from cipher text and replay attack. Also, the proposed protocol can parallelize the integrity function to

ISSN- 2350-0530(O), ISSN- 2394-3629(P)
IF: 4.321 (CosmosImpactFactor), 2.532 (I2OR)
InfoBase Index IBI Factor 3.86

increase system performance. [11], Hybrid Cryptosystem using AES and Hash Function, Vanishreeprasad S and Mrs K N Pushpalatha (June 2015) tells that Secure data communication is of a key concern in today's rapidly growing world. Various security mechanisms are developed in order to achieve the data security. Cryptography is one among them. It is the study of mathematical techniques that are related to the aspects of information security such as confidentiality, data integrity, authentication, and availability. The proposed architecture integrates the cryptographic algorithms, Advanced Encryption Standard algorithm (Symmetric) and the Hash function, SHA-2 to improve the data security to a greater extent. [1], Hybrid Cryptography by the Implementation of RSA and AES, Palanisamy V and Jeneba Mary A (April 2011) tells that the Rijndael algorithm mainly consists of a symmetric block cipher that can process data blocks of 128, 192 or 256 bits by using key lengths of 128, 196 and 256 bits. This work using Rijndael cryptography symmetric algorithm for data encryption/decryption and RSA cryptography asymmetric algorithm for Rijndael key's encryption/decryption. The encryption and decryption of any data has a secure key, which is used for data encryption. For this purpose asymmetric key is used. This work securing the data key using RSA algorithm. Here RSA key size is 128-bytes. This work also generating two pairs of keys; public and private key. Using Public key it encrypts the data key and other one is public and private key pair ,which will send to other person, so that opposite person can decrypt the encrypted key using his public and private key. [15], Two-phase hybrid cryptography algorithm for wireless sensor networks, Rawya R and Yasmin A (Nov 2015) [15] tells that For achieving security in wireless sensor networks (WSNs), Cryptography plays an important role. In this paper, a new security algorithm using combination of both symmetric and asymmetric cryptographic techniques is proposed to provide high security with minimized key maintenance. It guarantees three cryptographic primitives, integrity, confidentiality and authentication. Elliptical Curve Cryptography (ECC) and Advanced Encryption Standard (AES) are combined to provide encryption. XOR-DUAL RSA algorithm is considered for authentication and Message Digest-5 (MD5) for integrity. The results show that the proposed hybrid algorithm gives better performance in terms of computation time, the size of cipher text, and the energy consumption in WSN. It is also robust against different types of attacks in the case of image encryption.

From the survey of papers various authentication schemes like hybrid cryptography, AES, RSA and ECC schemes are discussed and their problems are identified. Finally to secure the network from the attack due to malicious nodes misbehaviour, hybrid cryptography using AES and ECC algorithms are chossen. Since hybrid cryptography is fast and efficient, it doesn't required lengthy procedure, identification, and detection of malicious nodes misbehaviour can be done in a simple way.

4. Existing System

In this existing system, they have designed a protocol called FBeeAdHoc. This protocol acts as a security framework to another protocol called BeeAdHoc protocol. This framework uses fuzzy set theory and digital signatures. The fuzzy logic is used to calculate the evaluated nodes trust value. Digital signatures are used to verify the integrity of routing information. BeeAdHoc protocol is a routing algorithm for energy efficient routing in mobile ad hoc networks. But a malicious node can seriously disrupt the routing behavior of this protocol. So that, this protocol has more security vulnerabilities.

ISSN- 2350-0530(O), ISSN- 2394-3629(P)
IF: 4.321 (CosmosImpactFactor), 2.532 (I2OR)
InfoBase Index IBI Factor 3.86

BeeAdHoc is a reactive source routing algorithm with effective energy for routing in MANETs, which has been inspired from bee behaviors. It uses two types of agents; scouts to discover new routes and foragers to transport data from source to destination. When anode is required to send data to a particular destination, the forward scout is broadcast on the network. The intermediate nodes that receive the scout, append their addresses in the source route of the scout until it arrives at the destination. When a forward scout reached on the destination, a backward scout is sent back to the source node using link reversal. Once a scout returns to its source node, it advertises the route to other foragers and then foragers transport data to the destination node. They collect the information about the network state and evaluate the quality of the traversed path.

4.1.Fbeeadhoc Protocol

In this section, security framework for BeeAdHoc which is designed based on fuzzy set theory and digital signature is represented.

4.2.Scout and Forager Authentication

When a source node has data to send to the destination, it first checks its dance floor to specify a forager for a data packet. If it finds one, then it uses the complete source route in forager for data packet transmissions. Otherwise, it broadcasts a forward scout to all its neighbors for discovering new routes to the destination node. This forward scout contains source ID, destination ID, source route and TVs appended by the intermediate nodes along the route. After the transmission of any forward scout, the sender puts itself in promis-cuous mode and calculates the trust value of evaluated nodes by using the approach described above. When a node receives a forward scout, it can confirm that the forward scout not been modified by a malicious node with the help of the list of node TVs. It appends its address in the source route and TV obtained from the upstream node on the route to the forward scout and retransmits it. When a forward scout reached to the destination, it contains the list of nodes and TVs of each hop along the route. The destination node computes Route Tv(P) for the route P by using formula. This value used to select the best route when more than one route is discovered and they have the equal hop count. Then the destination node unicasts the backward scout back to the source node and after transmitting computes the trust value of evaluated node. The pseudo codes of security for forward scouts and backward scouts are shown. Once the backward scout is received by the source node, it can verify that the backward scout have not tampered by a malicious node by using the list of node TVs. Then it recruits the foragers for transport data to the destination node. Similarly, after the transmission of forager, each node, computes the trust value of evaluated node. In this approach, to protect the routing information found by forager along the route, a sending node utilizes a digital signature that computes an authenticator as given by the equation

$$Auth_{RIi} = sign(H(routing\ information),\ keyP_i)$$

A receiving node uses the verification function to confirm the integrity of routing information, as given by the equation

$$Verify(Auth_{RIi}\ ,\ H(routing\ information),\ keyU_i)$$

ISSN- 2350-0530(O), ISSN- 2394-3629(P)
IF: 4.321 (CosmosImpactFactor), 2.532 (I2OR)
InfoBase Index IBI Factor 3.86

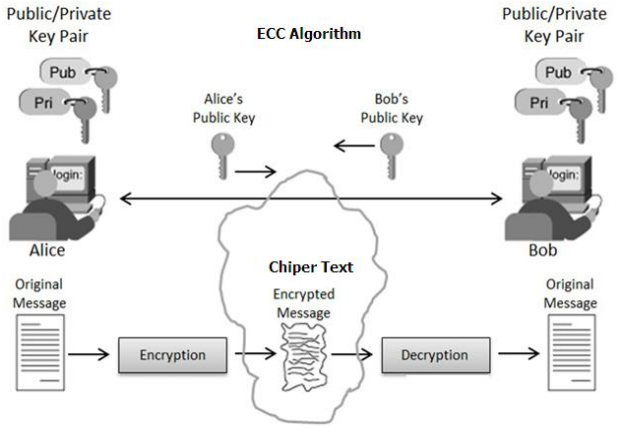
In which, *H(M)* represents hash of message *M* and $keyP_i$ and $keyU_i$ represent private key and public key of node *i*.

5. Problem Identification

In Existing system, FBeeAdHoc protocol provides the authentication of routing information using DSA/SHA1 algorithms. This security mechanism provides only the authentication of routing information; it doesn't provide the security of routing information to avoid further modification of routing information. DSA algorithm gives increased routing overhead, minimum routing effectiveness and increased routing delays. It provides signature file size and key size around 89 byte and 1024 bits respectively. So that, the total output size becomes large compared to other security mechanism. The security provided by the DSA/SHA1 algorithms are not sufficient for the Wireless Ad Hoc networks.

6. Proposed Method

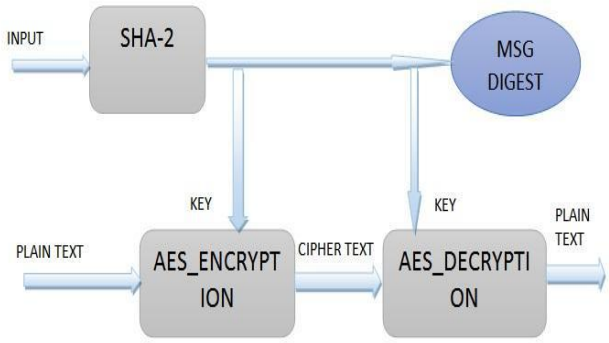
Mobile ad hoc network (MANET) is a group of mobile nodes that communicates with each other without any supporting infrastructure. These networks are vulnerable to several security threats. Malicious node can drop all or partial received packets instead of forwarding them to the next hop through the path. In order to find the malicious nodes, an initial transmission is made between the source and destination nodes. Using fuzzy rules, the trust value of each node is computed and it varies from 0 to 1. A common threshold value is set for each node and by using this threshold value, every node in the network can be identified as either a malicious node or a regular node. After identifying the malicious nodes, these nodes are eliminated by muting the power to off state. As the malicious nodes are eliminated between source and destination nodes, source node can select another trusted path to its destination node. For security and authentication of routing information, a hybrid cryptography is employed, using advanced encryption standard (AES) and elliptic curve cryptography (ECC) algorithms. AES algorithm is used as symmetric algorithm to encrypt the routing information and ECC algorithm is used as asymmetric algorithm to encrypt the public key. During encryption, the original plain text is converted into cipher text with encrypted public key and similarly during decryption cipher text is converted into original plain text with decrypted private keys. So the proposed method involves both AES and ECC algorithms which provides security mechanism as efficient and sufficient one.



ISSN- 2350-0530(O), ISSN- 2394-3629(P)
IF: 4.321 (CosmosImpactFactor), 2.532 (I2OR)
InfoBase Index IBI Factor 3.86

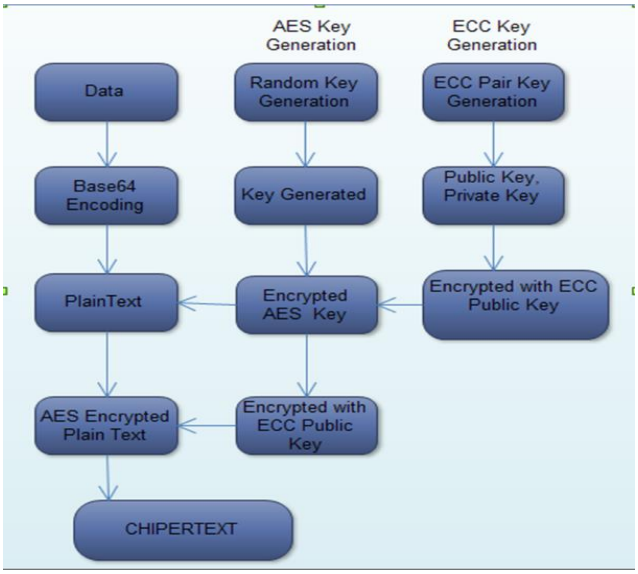
7. Hybrid Cryptosystems

A hybrid cryptosystem is one which combines the convenience of a public-key cryptosystem with the efficiency of a symmetric key cryptosystem. Here, we propose a provably two way secured data encryption system, which addresses the concerns of user's privacy, authentication and accuracy. This system has two different encryption algorithms have been used both in the Encryption and decryption sequence. One is public key cryptography based on linear block cipher another one is private key cryptography based on simple symmetric algorithm. This cryptography algorithm provides more security as well as authentication comparing to other existing hybrid algorithm.



7.1.Sender Side Encryption Module

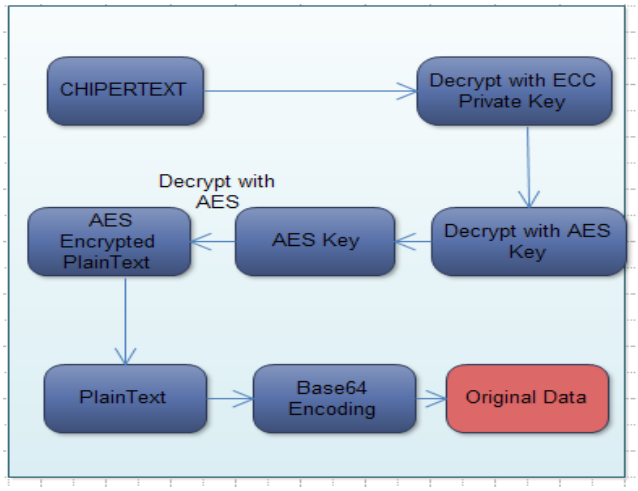
In sender side, the routing information file is encrypted using AES algorithm with the help of symmetric private key. Key encryption is done using public key cryptography called ECC algorithm. At first, the data file is converted into plain text by using base 64 encoding. Then, it is encrypted with the AES encryption by using AES random private key. This symmetric key is encrypted using public key cryptography called ECC algorithm. The encrypted plain text along with the encrypted symmetric private key is combined to form a cipher text. Cipher text is an encrypted file which is send to the receiver.



ISSN- 2350-0530(O), ISSN- 2394-3629(P)
IF: 4.321 (CosmosImpactFactor), 2.532 (I2OR)
InfoBase Index IBI Factor 3.86

7.2.Receiver Side Decryption Module

In receiver side also, two decryption processes is followed. At first, the decryption of symmetric private key from encrypted cipher text is done by using ECC private key decryption. After this symmetric private key is extracted from the cipher text. By using this symmetric key, the AES decryption of cipher text is done. After getting plain text, the base 64 decoding is done to get the original data file.



7.3.Advantages

By using this hybrid cryptography, we have the following advantages

- Reduced routing overheads and delays
- Reduced output file size
- Increase in space and bandwidth
- Improved routing effectiveness with more security
- Enhanced attackers detection and prevention

8. Conclusion

Secure routing in MANET is achieved through hybrid cryptosystems, where AES data encryption/decryption algorithm is used for data encryption and ECC key encryption algorithm is used as asymmetric key algorithm.

So the proposed secure algorithm provides more security compared to the existing secure algorithm. The parameter comparison of hybrid cryptosystems is done and it shows that the proposed algorithm is more efficient and reliable compared to our existing system.

References

[1] Palanisamy V, Jeneba Mary A, “Hybrid Cryptography By The Implementation Of RSA and AES”; International Journal of Current Research; vol.3, No.4, 2011, 241-244.

ISSN- 2350-0530(O), ISSN- 2394-3629(P)
IF: 4.321 (CosmosImpactFactor), 2.532 (I2OR)
InfoBase Index IBI Factor 3.86

[2] Shaikh A P, Kaul V, "Enhanced Security Algorithm using Hybrid Encryption and ECC"; Journal of Computer Engineering; Vol.16, No.3, 2014, 80-85.
[3] Bing Ji, Liejun Wang, Qinghua Yang, "New Version of AES-ECC Encryption System Based on FPGA in WSNs"; Journal of Software Engineering; Vol.9, No.1, 2015, 87-95.
[4] Xia H, Jia Z, Li X, Ju L, Sha EHM, "Trust prediction and trust-based source routing in mobile ad hoc networks", Journal of Ad Hoc Networks; Vol.11, 2012, 2096-2114.
[5] Wedde HF, Farooq M, Pannenbaecker T, Vogel B, "BeeAdHoc: an energy efficient routing algorithm for mobile ad hoc networks inspired by bee behavior"; Proceddings of ACM for Generation of Evolutionary Computing Conference, 2005, 153–60.
[6] Marjan Kuchaki Rafsanjani, Hamideh Fatemidokht, "FBeeAdHoc: A secure routing protocol for BeeAdHoc based on fuzzy logic in MANETs"; International Journal of Electricals and communications, 2015, 1-9.
[7] Singh G, kumar N, Verma A K, "ANTALG: An Innovative ACO based Routing Algorithm for MANETs", Journal of Networks and Computer Applications, Vol. 45, 2014.
[8] Sarkar S, Datta R, "A secure and energy-efficient stochastic multipath routing for self-organized mobile ad hoc networks", Journal of Ad Hoc Networks, 2015.
[9] Son T T, Minh H L, Sexton G, Aslam N, "A novel encounter-based metrice for mobile ad-hoc networks routing", Journal of Ad Hoc Networks, Vol.14, 2014.
[10] Saif Al-alak, Zuriati A, Azizol A, "AES and ECC Mixed for ZigBee Wireless sensor security", International Journal of Electrical, Computer, Energetic, Electronic and Communication Engineering, Vol. 5, Issue 9, 2011.
[11] Vanishreeprasad S, Mrs K N Pushpalatha, "Design and Implementation of Hybrid cryptosystem using AES and Hash Function", Journal of Electronics and Communication Engineering, Vol. 10, Issue 3, 2015.
[12] Kaliappan M, Paramasivan B, "Enhancing secure routing in Mobile Ad Hoc Networks using a Dynamic Bayesian Signalling game model", Journal of Computer and Electrical Engineering, 2015.
[13] Bing J, Liejun W, Qinghua Y, "New Version of AES-ECC Encryption System Based on FPGA in WSNs", Journal of Software Engineering, Vol. 9, Issue 1, 2015.
[14] Kim J, Tsudik G, "SRDP: Secure route discovery for dynamic source routing in MANETs", Journal of Ad Hoc Networks, Vol.7, 2009.
[15] Rawya R, Yasmin A, "Two-Phase Hybrid Cryptography for Wireless Sensor Networks", Journal of Electrical Systems and Information Technology, 2015.

*Corresponding author.
E-mail address: siva881155@gmail.com