AUSTRALIAN JOURNAL OF BASIC AND APPLIED SCIENCES

ISSN:1991-8178 EISSN: 2309-8414
Journal home page: www.ajbasweb.com

Data Protection in MANET Using Symmetric and Asymmetric Approaches

[1]A. Parvathavarthini and [2]Dr.S.S. Dhenakaran

[1]Ph.D Research Scholar Department of Computer Science Alagappa University – Karaikudi Tamilnadu-India-630003
[2]Professor Department of Computer Science Alagappa University – Karaikudi Tamilnadu-India-630003

Address For Correspondence:
A. Parvathavarthini, Ph.D Research Scholar Department of Computer Science Alagappa University – Karaikudi Tamilnadu-India-630003
E-mail-parvawin@gmail.com

ARTICLE INFO

Article history:
Received 18 June 2017
Accepted 28 July 2017
Available online 20 August 2017

Keywords:
MANET, Security, Symmetric Key, Asymmetric Key, Data Encryption, Data Decryption

ABSTRACT

Background: Collection of Wireless mobile nodes makes a network without any centralized base station is called Mobile Ad hoc Network (MANET). The MANET faces many challenges during sending data from one node to another node owing to the absence of the central base station. So, security is one of the challenges in MANET. Cryptography is more secure to transmit over insecure network. The traditional cryptographic techniques are well known and the attackers are known about the solution. Therefore new kind of cryptographic technique is required which improve the security and complexity of data cipher. **Objective:** Cryptography is an important for secure data communication. Encrypted data is more secure to transmit over insecure network and any unauthorized user won't be able to read the encrypted data if don't have the secret key to decrypt the message. The objective of this paper is to propose a secure message communication using hybrid approach to send the message securely from one to node to another node. This paper uses both symmetric key and asymmetric key (or public key) (Paillier) algorithm for secure data encryption. **Result:** The performance of the proposed method has been evaluated through experimental results. The proposed work is compared to the existing encryption algorithms (DES and RSA) with encryption and decryption time. The experimental result shows that proposed work has better results compared to other methods. **Conclusion:** Data confidentiality is important security requirement in ad-hoc network. This cryptography algorithm provides more security as well as authentication comparing to other existing algorithm**.** The analysis indicates that the suggested algorithm is suited for energy constrained wireless sensor networks. The result of the proposed work shows that processing time is more efficient compared to other algorithms.

INTRODUCTION

Ad-hoc networks are particular category of wireless networks without any preset infrastructure or centralized administration. A Wireless Sensor Networks comprised of resource constrained sensor nodes that are densely deployed in a unattended environment (Yick *et al*., 2008). The sensor nodes collect data from the physical phenomena which occur in the environment, process it and transmit the sensed data via wireless signals to the base station. A base station is power rich node among all sensor nodes in WSNs. Sensor nodes are typically categorized by low-cost, low-power, multifunctional, low bandwidth, small memory sizes and limited energy. Due to these characteristics WSN ensures a broad range of applications in areas such as military, health, environment, commercial and agriculture. Consequently, securing this kind of network becomes a most critical task (Al Ameen *et al*., 2012).

Some challenges of security maintenance in ad-hoc network: (Yu *et al*., 2011) First, security attacks on data communication, such as passive eavesdropping, packet injection or even violations of confidentiality are widespread. Second existing security protocols that are based on a centralized or infrastructure-based network environment will not work in this mobile environment. Third, in order to achieve better network throughput in

To Cite This Article: A. Parvathavarthini and Dr.S.S. Dhenakaran., Data Protection in MANET Using Symmetric and Asymmetric Approaches. ***Aust. J. Basic & Appl. Sci.,*** *11(11): 103-110, 2017*

such a highly dynamic environment, the default routing protocol does not implement any security protection during end-to-end communication.

Data security is one of the main issues in ad hoc networks. The cryptographic mechanism is used to provide the data security. Cryptography is one of the primary techniques used for securing information while message communication (Stallings, 2013). Cryptography techniques provide confidentiality, authentication, and integrity of the message. There are two types of cryptographic techniques which are mostly used i.e. symmetric cryptography and asymmetric cryptography.

Symmetric key cryptography uses the same key for encryption as well as decryption thus making it faster compared to Asymmetric Key cryptography which uses different keys for encryption and decryption. Symmetric cryptography is also known as secret key of private key cryptography. DES and AES is example of symmetric key cryptography algorithm. Asymmetric cryptography is also known as public key cryptography. RSA and ECC is example of asymmetric key cryptography. The symmetric cryptography technique provides a suitable amount of security, but maintenance of keys is difficult. On the other hand, in asymmetric algorithms maintenance of keys is easier, but they offer a lesser level of security (Mohindru and Singh, 2016).

This paper combines symmetric and asymmetric key cryptography to propose a hybrid cryptography technique that provides high data protection in Ad hoc network. The data was encrypted twice for improving the data security. The paper is organized as follows: Section II discussed the related work. Section III gives the objectives of the research work. Section IV introduced the proposed algorithm for securing the message communication within Ad hoc network. Section V presents the analysis of proposed algorithm. At last, we conclude our work in section VI.

Related Work:

A MANET is a rapidly growing technology which is based on a self-organized and rapidly deployed network. Due to its great features, it attracts different real world application areas where the networks topology changes very quickly. However, in many researchers are trying to remove it main weaknesses such as battery power, computational power, security and limited bandwidth. Thus a lot of works under progress in this subject particularly routing attacks and its existing countermeasures. The existing security solutions of wired networks cannot be applied directly to MANET, which makes a MANET much more vulnerable to security attacks. In this chapter some researchers existing works are reviewed.

Shashi *et al*., (2011) proposed a modern review of comparative analysis of encryption algorithms like AES, DES and RSA for data communication by using memory usages, encryption time, battery power and output bytes. Based on text files used and the experimental result it was concluded that DES algorithm consumes least encryption time and AES algorithm has least memory usage while the difference in encryption time is very minor in case of AES and DES algorithms. RSA consumes longest encryption time, high memory usage and less output byte.

Gurjeevan Singh *et al*., (2011) studied throughput analysis of various selected encryption algorithms like AES, DES, 3DES and Blowfish. The simulation results shows the Blowfish Algorithm has better performance than other algorithms followed by AES in terms of throughput and 3DES has least performance than others.

Gurjeet Singh (2011) proposed the security threats and maintain in MANET. Ad hoc networks present different threats due to their very different properties. These properties open up very different security risks from conventional wired networks, and each of them affects how security is provided and maintained. Ad hoc networks are generally more prone to physical security threats than are fixed cable networks. Existing link security techniques are often applied within wireless networks to reduce security threats. As a benefit, the decentralized nature of the network control in Ad hoc networks provides additional robustness against the single points of failure of more centralized approaches.

Aman (2012) proposed trust formalization in MANET within multichannel. This would be helpful in establishing keys in the network and nodes can communicate data securely without any delay in MANETs. Due to this problem like transmission delay, security can be solved to achieve better performance of QOS and throughput. We provide an overview of routing schemes proposed for ad hoc mobile networks. In which make the comparison between AODV and DSR routing protocol performance for transmission.

Amandeep Makkar *et al*., (2011) studied a behavioral study of MANET routing protocols. In this research paper, an effort has been made to concentrate on the behavioral study and performance analysis of various prominent routing protocols like DSDV, DSR, TORA, and AODV on basis of quantitative and qualitative metrics. Based on performance analysis, recommendations have been made about the significance of either protocol under different circumstances and the analysis concludes that both protocols are good in performance in their own categories. More over due to dynamically changing topology and infra structure less property, secure and power aware routing is hard to achieve in MANETs.

Australian Journal of Basic and Applied Sciences, 11(11) August 2017, Pages: 103-110

Research Objective:

Data Security is one of the key issues addressed by ad hoc networks. Through cryptographic encryption methods, one can prevent a third party from understanding transmitted raw data over unsecured channel during transmission. The cryptographic methods for enhancing the security of digital contents have gained high significance in the current era. Breach of security and misuse of confidential information that has been intercepted by unauthorized parties are key problems that information security tries to solve. This paper sets out to contribute to the general body of knowledge in the area of classical cryptography by developing a new hybrid way of encryption of plaintext.

Hybrid cryptography is a blend of symmetric and asymmetric cryptography. The symmetric cryptography technique provides a suitable amount of security, but maintenance of keys is difficult. On the other hand, in asymmetric algorithms maintenance of keys is easier, but they offer a lesser level of security. The limitations of symmetric-key cryptographic techniques were resolved by the asymmetric cryptographic technique. Therefore when combined form of these cryptography techniques is used in the Ad hoc networks, they out come with a new technique which is more resilient against the attacks and hence retain the high degree of data security.

Methodology:

The prime motive of our proposed algorithm is to secure message communication Ad hoc network. The algorithm makes use of the hybrid cryptography algorithm. Our algorithm claim to offer high level of data security, consumes less energy and low computational overhead.

The network consists of N number of Nodes. Each node within the network maintain information related to unique ID, location, neighbor list (id, location) corresponding to each 1-hop neighbors.

The nodes are not tamper-resistant. Attacker compromises the nodes, which in turn releases all its security information to it. The message was protected before they send.

Figure1 shows the encryption and decryption structure of our proposed algorithm.

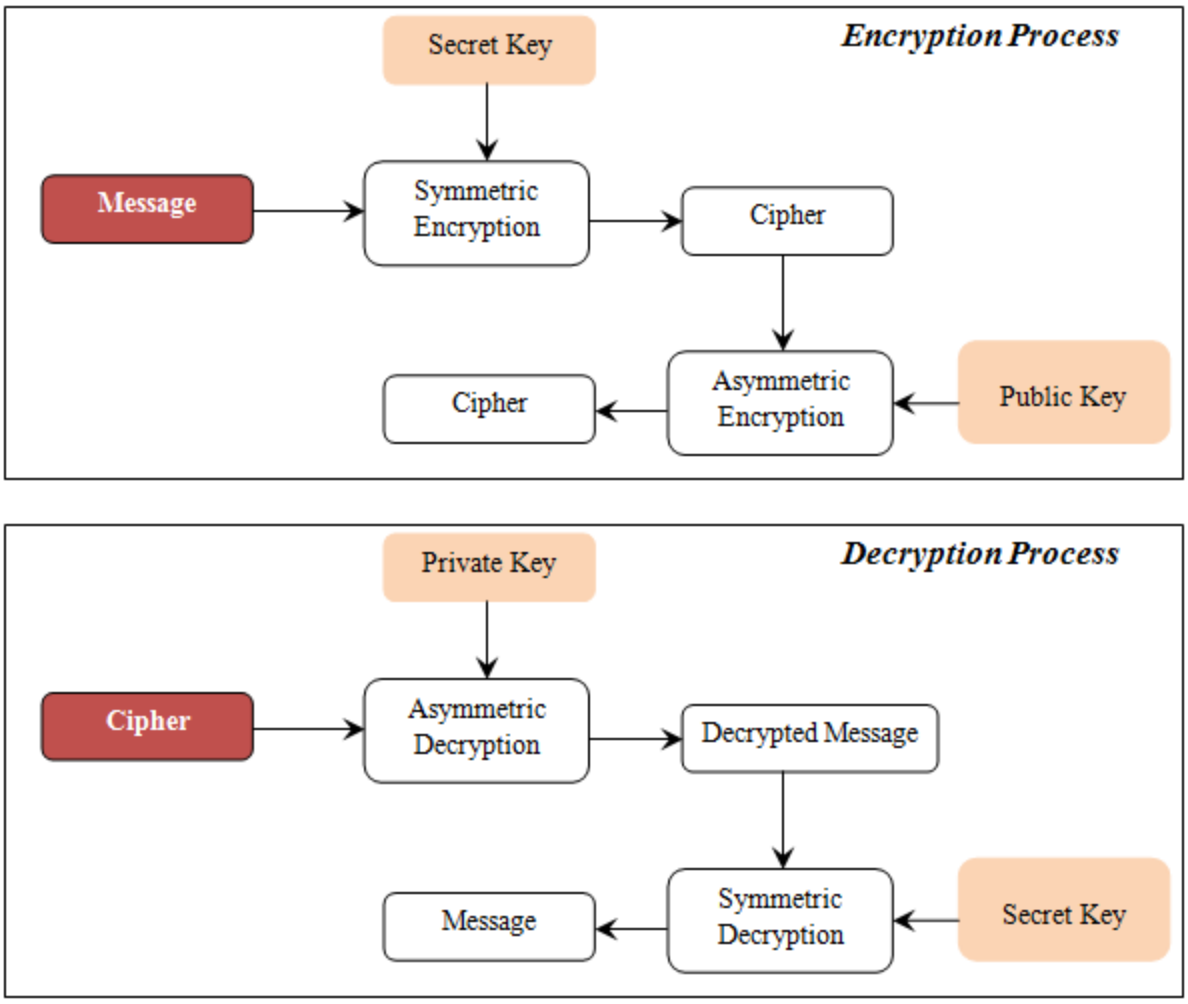

Fig. 1: Encryption and Decryption Process

Australian Journal of Basic and Applied Sciences, 11(11) August 2017, Pages: 103-110

The Source node (S) wants to send the message (M) to Destination node (D). Therefore, the source node first encrypts the message (M) using symmetric key encryption (SKE). It returns the cipher text (C1) of original message (M). Next, the cipher text (C1) is encrypted using Asymmetric key encryption (ASKE). The encrypted cipher text (C2) is send to Destination Node.

The Destination Node receives the cipher text (C2) and it first uses Asymmetric key decryption to decrypt the cipher text (C2). After that it uses symmetric key decryption to get the original message (M).

The following section explains the symmetric and asymmetric key encryption and decryption algorithm.

Symmetric Key Encryption and Decryption:

Key Generation

Initialize the generator g=3;
Select random number r
Get Message Length mlen
Secret Key = (g,r,mlen)

Encryption

Compute n = 2*r + mlen;
Initialize the finite field

(Finite Field contains a finite number of elements. As with any field, a finite field is a set on which the operations of multiplication, addition, subtraction and division are defined and satisfy certain basic rules)

Initialize an array m with n size. (It contains original message)
Initialize an array C with n size. (It contains cipher text)
for i = 0; i < n; i++
FiniteField cur = new FiniteField(1);
FiniteField tot = new FiniteField(0);
For j = 0; j < n; j++
A[i][j] = cur.val;
tot = cur.mult(m[j]).add(tot); // Multiplication and Addition Operation
cur = cur.mult(wn);
end
wn = wn.mult(g);
c[i] = tot.val;
end

Decryption

Get Secret Key = (g,r,mlen)
Get array of cipher text C
for i = 0; i < n; i++)
FiniteField cur = new FiniteField(1);
for j = 0; j < mlen; j++
A[cnt][j] = cur.val;
cur = cur.mult(wn);
end
c[cnt] = C[i];
cnt++;
if(cnt >= mlen)
break
end
end

Asymmetric Key Encryption and Decryption:

Key Generation

Choose two large prime numbers p and q randomly and independently of each other such that gcd(pq,(p-1)(q-1))=1

Compute n=p*q and λ=lcm(p-1,q-1)
Initialize the generator g=2;

Calculate, modular multiplicative inverse $\mu = \left(L\left(g^{\lambda} \bmod n^2\right)\right)^{-1} \bmod n$

Where L is defined as $L(u) = \dfrac{u-1}{n}$

The Public Key is (n, g)
The Private Key is (λ, μ)

Encryption
Let m be a message
Select random r
Compute cipher text $c = g^m \cdot r^n \bmod n^2$
Decryption
Decrypt message $m = L\left(c^{\lambda} \bmod n^2\right) \cdot \mu \bmod n$

Figure 2(a) shows the sender node processing and Figure 2(b) shows the destination node processing.

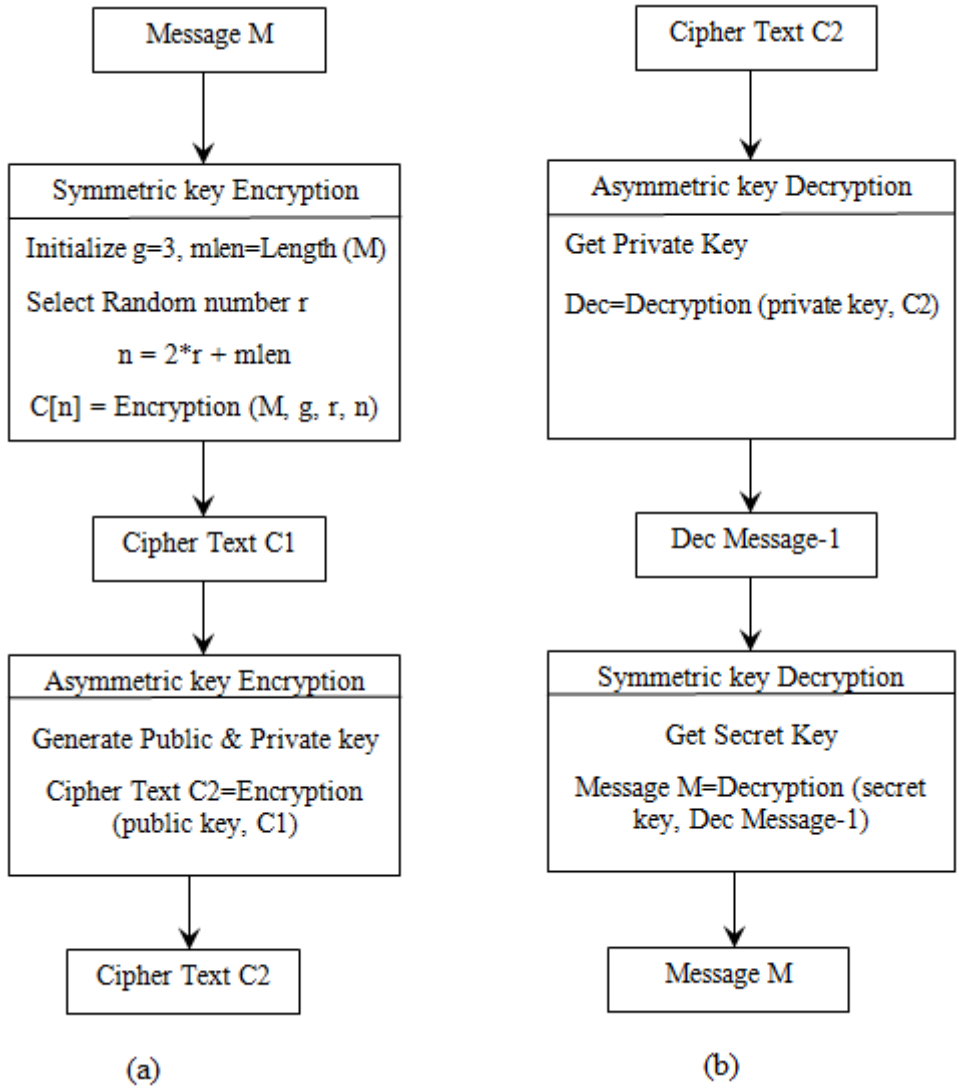

Fig. 2: Encryption and Decryption Process of Source Node and Destination Node

RESULT AND DISCUSSION

The effectiveness of any cryptographic algorithm depends on mainly two factors, one is the encryption / decryption methods and another key is used. The proposed algorithm uses the hybrid approach, including the symmetric key and asymmetric key algorithm which make the proposed algorithm more robust and cannot be easily attacked the message.

The message is encrypted by symmetric key algorithm is faster than the asymmetric key algorithm which are complicated and secure. Therefore the symmetric key algorithm has low computational overhead and low communication overhead and the asymmetric key algorithm has high security and low storage overhead.

Example:

This section gives an example of message encryption and decryption

Consider the message "*Data security is one of the main issues in ad hoc networks*"

Encryption in Source Node:

The given message is encoded using symmetric key encryption

The length of the message (mlen) = 58 bytes

Select Random number r = 5

Generate the encoded message length n = 2*r + mlen

n = 2*5 +58

n = 68 (length of encoded messages)

After applying symmetric key encryption, the original message is encoded as,

5, 134, 182, 92, 217, 49, 36, 9, 14, 7, 51, 190, 255, 40, 211, 37, 183, 217, 244, 73, 76, 194, 190, 62, 141, 59, 215, 200, 20, 97, 157, 213, 88, 207, 195, 230, 55, 97, 200, 244, 107, 85, 45, 202, 239, 26, 183, 220, 171, 166, 130, 220, 116, 159, 76, 187, 245, 82, 4, 10, 135, 119, 203, 15, 216, 241, 185, 174

The encoded message is encrypted using asymmetric key encryption,

18522, 258633, 219113, 208886, 260103, 160601, 47703, 12263, 108327, 74088, 74226, 127395, 249700, 195070, 8503, 95406, 154137, 260103, 123856, 91740, 165742, 49697, 127395, 27233, 150700, 251982, 136048, 55629, 114792, 150305, 205204, 34012, 190611, 18287, 99394, 96276, 51260, 150305, 55629, 123856, 220171, 201382, 276371, 222516, 145915, 244463, 154137, 92201, 153110, 235607, 282498, 92201, 228308, 252638, 165742, 193480, 247712, 96195, 9261, 24526, 233177, 121930, 160943, 216654, 272096, 15482, 48370, 88524

The encoded message is send to destination node.

Decryption in Destination Node:

The destination node receives the encrypted message. First it decrypts the message using asymmetric key decryption. The decrypted message as follows:

5, 134, 182, 92, 217, 49, 36, 9, 14, 7, 51, 190, 255, 40, 211, 37, 183, 217, 244, 73, 76, 194, 190, 62, 141, 59, 215, 200, 20, 97, 157, 213, 88, 207, 195, 230, 55, 97, 200, 244, 107, 85, 45, 202, 239, 26, 183, 220, 171, 166, 130, 220, 116, 159, 76, 187, 245, 82, 4, 10, 135, 119, 203, 15, 216, 241, 185, 174

To get the original message, the decrypted message was decoded using symmetric key decryption.

The destination node gets the decrypted message as, "*Data security is one of the main issues in ad hoc networks*"

The proposed algorithm is compared with RSA-3DES and RSA-AES algorithm.

Table 1 Execution of Encryption Time

File Size in KB	Encryption Time in MS		
	RSA-3DES	RSA-AES	Proposed
1	303	327	125
5	468	624	312
10	733	810	561
25	1732	1826	1576
50	3556	3759	3291
75	5803	6287	5663
100	8221	8502	7675

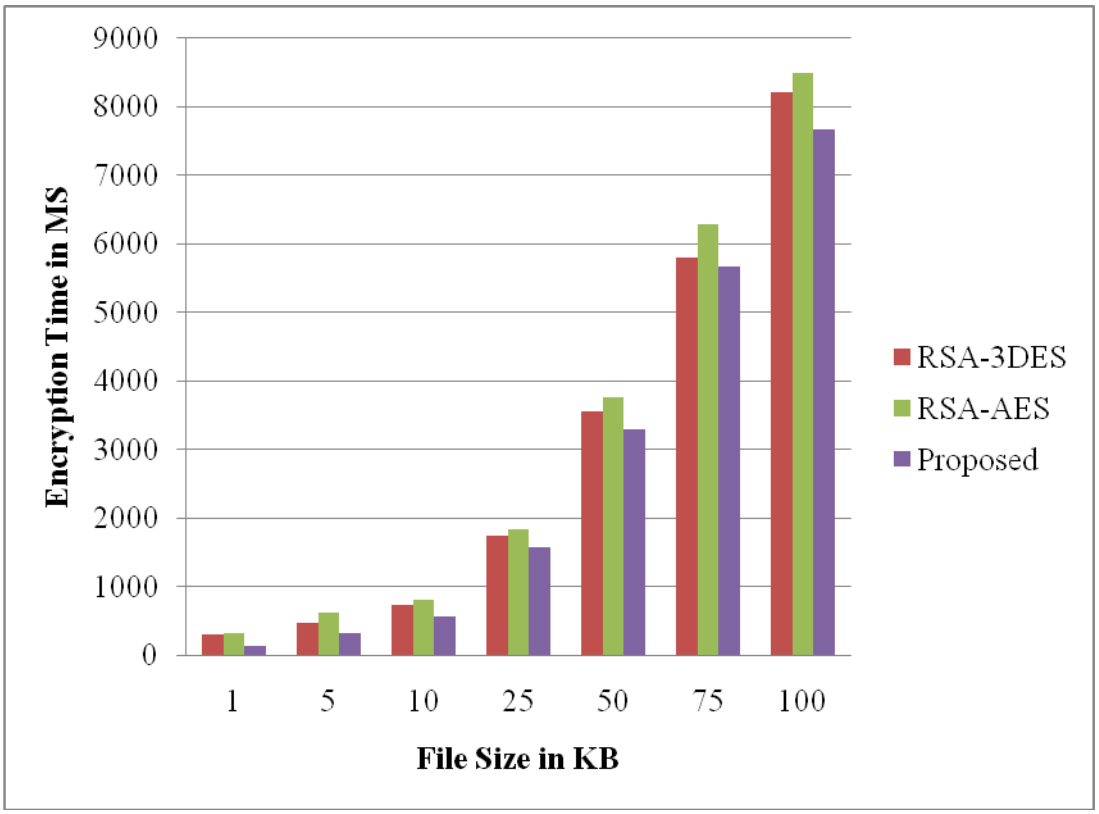

Figure 3 shows the Execution time of Encryption

Conclusion:

Data confidentiality and privacy are the two most important security requirements in ad-hoc networks. Most security mechanisms rely on data encryption, which is a message combined with a secret key to generate a cipher text that cannot be revived without the original key. This encryption mechanism can prevent any unauthorized user from gaining access to the secured communication. Maintaining security in the highly dynamic ad-hoc wireless network is full of challenges due to malicious nodes. In this paper, an efficient algorithm is proposed to secure message from being modified by the malicious node. The algorithm first uses the symmetric key encryption to produce the cipher text. Then the asymmetric key algorithm is used to generate the second level of encrypted message. By using the hybrid cryptography algorithm the network security increases double times in terms of confidentiality. The malicious node cannot decrypt the message. From the performance analysis, it can be reasoned that the proposed algorithm provides low computational overhead, low communication overhead and attain high level of security. The encryption and decryption time of proposed algorithm is compared to DES and RSA algorithm. The data execution time was compared to multiple hybrid algorithms. From the results the proposed hybrid algorithm takes lesser time to execute the encryption and decryption. The cipher text of original message cannot be decrypted by the malicious nodes. As the future extension, this algorithm would be simulated using the simulator and can be applied to real world application to check the performance and include the intrusion detection in MANET.

REFERENCES

Al Ameen, M., J. Liu, K. Kwak, 2012. Security and privacy issues in wireless sensor networks for healthcare applications. Journal of Medical Systems, 36(1): 93-101.

Aman deep Kaur, 2012. Trust Formalization in MANET Within Multichannel. International Journal of Emerging Technology and Advanced Engineering (IJETAE), ISSN 2250-2459, 2: 6.

Aman deep Makkar, Bharat Bhushan, Shelja and Sunil Taneja, 2011. Behavioral Study of MANET Routing Protocols. International Journal of Innovation, Management and Technology, 2: 3.

Gurjeet Singh, 2011. Security Threats and Maintenance in Mobile ad hoc networks. IJECT, 2: 3.

Gurjeevan Singh, Ashwani Kumar Singla and K.S. Sandha, 2011. Throughput Analysis of Various Encryption Algorithms. IJCST, 2: 3.

Kuppuswamy, P., Q. Saeed, Y. Al-Khalidi, 2014. Hybrid Encryption/Decryption Technique Using New Public Key and Symmetric Key Algorithm. MIS Review, 19(2): 1-13.

Mohindru, V., Y. Singh, 2016. Efficient approach for securing message communication in wireless sensor networks from node clone attack. Indian Journal of Science and Technology, 9(32): 1-7.

Shashi Mehrotra Seth and Rajan Mishra, 2011. Comparative Analysis of Encryption Algorithms for Data Communication. IJCST 2: 2.

Stallings, W., 2013. Cryptography and network security: principles and practices, 5th(edn) Prentice-Hall.

Yick, J., B. Mukherjee, D. Ghosal, 2008. Wireless sensor net-work survey. Journal of Computer Networks, 52(12): 2292-2330

Yu, P.H., & U.W. Pooch, 2011. Security and dynamic encryption system in mobile ad-hoc network. IntechOpen, 23: 470-490.