International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395 -0056
Volume: 04 Issue: 03 | Mar -2017 www.irjet.net p-ISSN: 2395-0072

SECURITY IN MANETS USING CRYPTOGRAPHY ALGORITHMS

N Neelima[1], Lekharaju Sai Siddhartha[2], Chavali Meghana[3], Shaik Sameer[4], Shaik Ashika[5], Vemulamada Naga Chandramouli[6]

[1] Assistant Professor, [2,3,4,5,6] Final year B. Tech, Department of Information Technology, VRSEC, Vijayawada, India

---

Abstract - *Mobile Ad-hoc Network (MANET) is an important field where many of the users are using mobile devices for last few years where ad-hoc routing in networks is one of the prominent issues. A malicious node can drop the routing information, data packets intentionally and disturb the process of the routing protocol. To solve this problem, we proposed a novel approach for effective key management, and prevention of malicious nodes. Security to the routing protocol is incorporated using traditional SHA algorithm along with symmetric and asymmetric key encryption methods. The performance of the proposed algorithms is analyzed with different algorithms and results are shown improvement in terms of the time taken to transfer the data, communication overheads and battery consumption.*

Key Words: **MANETS, Security, Symmetric key cryptographic algorithm, Asymmetric key cryptographic algorithm, SHA, RSA, AES.**

1. INTRODUCTION

Now-a-days the mobile devices are used more frequently as every person owns at least a mobile device. We use these devices for almost everything like to share data, post an update, and share the information. In such cases these devices must be secured. Cryptography will be playing a major role in hiding the data or information. These cryptography algorithms are divided into two types, symmetric key cryptography algorithms and asymmetric key cryptography algorithms. The symmetric algorithms will use same key for encryption and decryptions of the information. These are again divided into Block ciphers and stream ciphers. Block ciphers will use block of data for the encryption and decryption like AES, DES and Blowfish. Stream ciphers use single bit at a time like in RC4. In asymmetric key algorithms, there will be two different keys used for the encryption and decryption, one is public key and another is private key. We can use one key for encryption and other for decryption like RSA algorithm. Public key is public to all but private key is recognized for the user only. Due to large processing of the keys the asymmetric algorithms are much slower than the symmetric key algorithms.

1.1 Goals of Cryptography

1.1.1 Confidentiality: Confidentiality is basically used to ensure that the data is safe and private this is obtained using encryption.

1.1.2 Data Integrity: This is to ensure that the data is not changed intentionally or accidentally.

1.1.3 Authentication: Authentication is to ensure that the originator is original and is known to receiver.

1.1.4 Non-Repudiation: Non-Repudiation is to assure that the sender cannot refuse the fact that he send the message or vice versa.

1.2 Asymmetric Key Algorithm

In asymmetric key algorithm two different keys are used, one public key and another private key. Generally, the public key is used for the encryption process and the private key is used for the decryption process because this will make only the receiver to decrypt the message. So, the sender encrypts the message with the help of the public key of the receiver and sends the message, now the receiver will be able to decrypt the message using his own private key.

1.3 Symmetric key Algorithm

In symmetric key algorithm, we will use only one single key for both encryption and decryption. The sender will encrypt the message with a secret key that is shared between the sender and the receiver privately. This key will be used by the receiver to decrypt the cipher text from the sender. Thus in this algorithms one secret key is used.

1.4 Cryptographic hash functions

The cryptographic hash functions are the functions that take an input and return a fixed-size alphanumeric string. The string is called the hash value or message digest or digital fingerprint or digest or checksum.

The ideal hash function has three main properties: (a) It is extremely easy to calculate a hash for any given data. (b) It is extremely computationally difficult to calculate an alphanumeric text that has a given hash. (c)It is extremely

unlikely that two slightly different messages will have the same hash.

A cryptographic hash function should behave as much as possible like a random function while still being efficiently computable. A cryptographic hash function is considered "insecure" from a cryptographic point of view, if either of the following is computationally feasible, finding a (previously unseen) message that matches a given hash values and finding "collisions", in which two different messages have the same hash value.

2. LITERATURE SURVEY

In [1] it is concluded that AES is faster and more efficient than other encryption algorithms. When the broadcast of data is considered there is insignificant difference in performance of different symmetric key schemes. Under the scenario of data transfer it would be better to use AES scheme in case the encrypted data is stored at the other end and decrypted multiple times.

In 2016, Madumita Panda has done performance analysis of encryption algorithms for security. In this paper, the professor compared different algorithms in terms of CPU time, memory, the algorithms include symmetric as well as asymmetric algorithms.

In 2014, Suni kumar Sahu, Ajay kushwaha have done analysis of symmetric encryption algorithms for mobile ad hoc network. In this paper, he compared only symmetric key algorithms in the MANETS and displayed the results in terms of battery usage, end to end delay, processing time etc. The author used ns2 simulator to compare the performance of the algorithms.

In 2016, M V Narayana, Dr G Narsimha, Dr SSVN Sarma proposed security enhancement in MANETS using SHA Algorithm [6]. In this paper, the authors proposed a method to improve the security in the mobile ad hoc networks using the Secure Hashing Algorithm.

In [2] it states that AES is faster and more proficient than other encryption algorithms. Increasing the key size by 64 bits of AES leads to increase in energy consumption about8%without any data transfer. The difference is not obvious. Reducing the number of rounds leads to power savings but it makes the protocol insecure for AES and should be avoided.

3. PROPOSED SYSTEM

The proposed system involves a multi-level security in MANETS where the data is will undergo the cryptographic hash function and an encryption algorithm and is sent to the destination where the data is decrypted and the data is checked for its integrity using the SHA algorithm.

At the sender the message digest of the data that has to be sent is obtained using the SHA-256 algorithm, then the data along with the message digest is encrypted and will be transmitted to the destination. When the message is received at the destination it will be decrypted and the hash code value of the incoming message is compared to the value that is concatenated to the input string. This way the integrity of the message is verified.

Now AES algorithm and RSA algorithms are used in the place of the encryption algorithms and their performance is compared.

3.1 SHA-256:

SHA-256 belongs to the SHA-2 family of hash functions; the family consists of SHA-256 and SHA-512 that are differentiated by the word block sizes. The FIPS PUB 180-2 standard is followed by the SHA-256. This is developed by the National Institutes of Standards and Technology (NIST) and other government and private parties.

A hash function is a mathematical function that converts the input valued into another compressed value of fixed length. The input to the hash function is of arbitrary length but output is of fixed length.

SHA-256 operates in the manner of MD4, MD5 and SHA-1. The message is first padded with its length in such a way that the result is a multiple of 512 bit long word then it is parsed into 512-bit message blocks $M_1, M_2 \ldots M_n$. Now the blocks are processed one at a time beginning from the initial buffer H (0), sequentially calculate

$$H(i) = H(i-1) + C_{Mi*}(H(i-1))$$

Where C is the SHA-256 compression function and + means word-wise mode 2^{32} addition. H(n) is the hash or message digest of the message

3.2 RSA Algorithm

RSA is the acronym derived for Ron Rivest, Adi Shamir and Leonard Adleman, who first described it in 1978. This algorithm is used to encrypt and decrypt the messages. It is an asymmetric cryptographic algorithm means it uses two different keys for encryption and decryption.

The main steps in the RSA algorithm are (a) Key Generation (b) Encryption (c) Decryption. The key generation can be done as follows: Generate two large prime numbers p and q of approximately equal size. Find the product of the two numbers let it be 'n'.

$$n = p*q$$

Calculate ϕ such that ϕ = (p-1)*(q-1). Next choose 'e' such that

gcd(e, ϕ) = 1 , 1 < e < ϕ

Compute the value d such that ed = 1 mod ϕ

Now the Message is encrypted like

Cipher = (Message ^{e}) mod n

The cipher message is then decrypted like

Message = (Cipher ^{d}) mod n

3.3 AES Algorithm

The Advanced encryption standard is symmetric key cryptographic algorithm which is also known as Rijndael. This is a block cipher algorithm used as an encryption standard by the U.S. government. This is the enhancement of the DES algorithm; AES is found at least six times faster than the DES algorithm.

AES algorithm uses 10 rounds for 128-bit keys, 12 rounds for 192-bit key and 14 rounds for the 256-bit keys where each of these rounds uses a different 128-bit round key which is calculated from the original AES key.

The encryption in AES is done as follows: (a) Byte Substitution (b) Shift rows (c) Mix columns (d) Add round Key. Now the initial message is converted into a non-readable format (cipher).

The decryption process is similar to the encryption process but the order of the operations is reverse i.e. (a) Add round key (b) Mix columns (c) Shift rows (d) Byte substitution.

The encryption and the decryption process needs to be separately implemented although they are very similar to each other.

4. RESULTS

The home page of the project is the following which allows you to choose the number of nodes to be created in the MANET

Fig -1: Home Screen

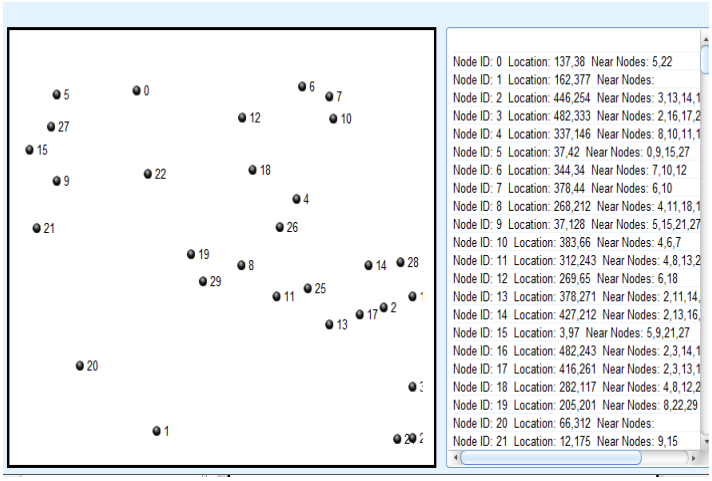

Fig -2: Mobile nodes Simulation

The data is then transferred from the source to destination with the SHA algorithm and AES algorithm.

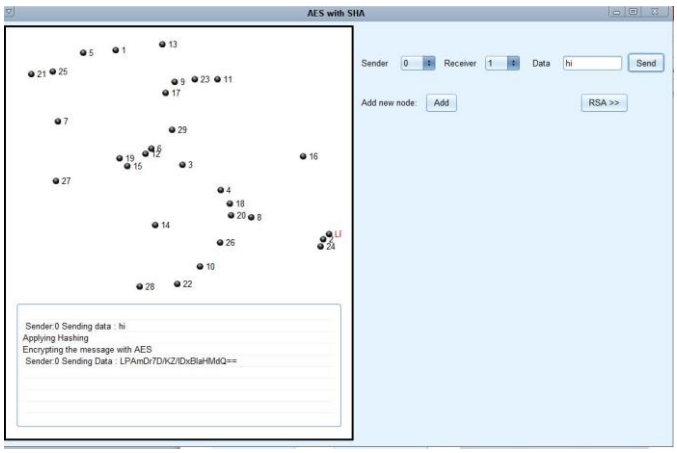

Fig -3: AES with SHA

Now the data is transferred using the RSA algorithm and SHA algorithm

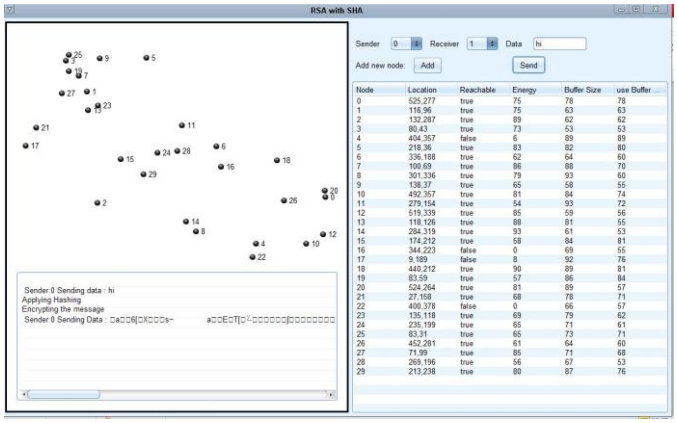

Fig -4: RSA with SHA

Finally the time and the battery consumptions of both the techniques are compared and the results are shown below:

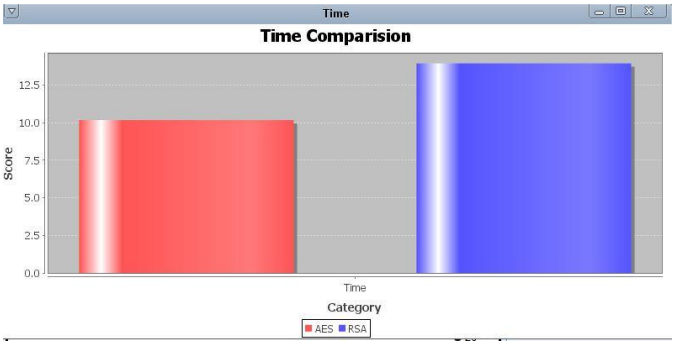

Fig -5: Time comparisons for AES with SHA and RSA with SHA (in seconds)

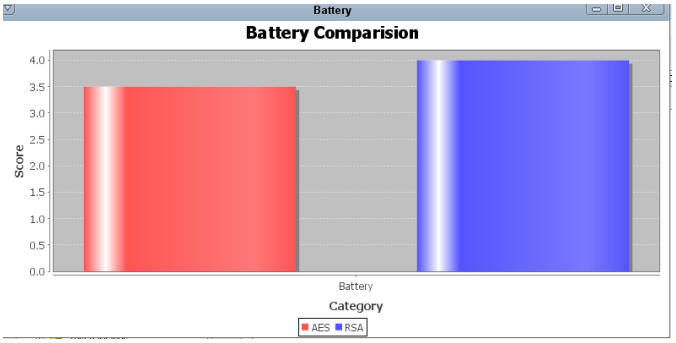

Fig -6: Battery comparisons for AES with SHA and RSA with SHA

5. CONCLUSIONS AND FUTURE WORK

The RSA algorithm will consume more time because of the large processing of the information. This makes the AES algorithm faster that the RSA algorithm. The battery consumption factor is also high for the RSA algorithm because of the calculation of the large primes and operations on them. This leaves that the AES along with the SHA shows better results than the RSA along with the SHA.

In future these algorithms will become obsolete as the advancement of the mobile processing technology and the introduction of highly advanced processing machines like super computers and quantum computers. So the security in these MANETS are to be provided by the future proof algorithms rather than algorithms that are vulnerable to brute force attacks in the future.

REFERENCES

[1] Nagesh Kumar, Jawahar Thakur, Arvind Kalia on "Performance Analysis Of Symmetric Key Cryptography Algorithms: DES, AES And Blowfish —in An International Journal of Engineering Sciences ISSN: 22296913 Issue Sept 2011, Vol.4, pp.28-37.

[2] S.Hirani, ''Energy Consumption of Encryption Schemes in Wireless Devices Thesis,'' university of Pittsburgh, April 9, 2003. Retrieved October 1, 2008, at: portal.acm.org/ citation.cfm?id=383768.

[3] Tamimi, A Al; —Performance Analysis of Data Encryption Algorithms||, Oct 2008.

[4] Nadeem, Aamer; "A Performance Comparison of Data Encryption Algorithms", IEEE 2005.

[5] Ruangchaijatupon, P. Krishnamurthy,‟ Encryption and Power Consumption in Wireless LANs-N,"" The Third IEEE Workshop on Wireless LANs -September 27-28, 2001- Newton, Massachusetts.

[6] M V Narayana, Dr G Narsimha, Dr SSVN Sarma proposed "Security enchancement in MANETS using SHA Algorithm", 2016.

[7] W. Stallings. "Cryptography and Network Security": Principlesand Practice. Prentice Hall, 2nd edition, 1999.