Trust and Cluster Based Attribute Based Double Encryption Authentication Mechanism in MANET

V.Gowthami [1], R. Buvaneswari[2]

[1]M.Phil Scholar, Department of Computer Science,
Hindusthan College of Arts and Science,
Behind Nava India, Coimbatore-641 028, Tamil Nadu, India,
[2]Head of Department IT & CT,
Hindusthan College of Arts and Science,
Behind Nava India, Coimbatore-641 028, Tamil Nadu, India,

Abstract

Mobile adhoc network (MANET) is a wireless communication network with collection of nodes and have no specific structure and are able to determine the nearby node through lack of centralized control .due to this protecting data from multiple nodes becomes major important, existing work focus on key distribution and management scheme to make safety. In existing system propose a secure public key and public key based encryption and decryption algorithm such as RSA, AES to make more security in the MANET based system, it also uses an authentication service based trust model and a network model to prevent nodes from obtaining false public keys of the others while they present a malicious node in the networks. In all of the RSA ,DES based algorithm based on the public key when the user easily identified the private key by identification of the key values ,so still it becomes major issues in the protection of data from malicious nodes in the trust and cluster based model .To overcome these problems we proposed a double encryption and decryption based schema first the original user sends data was encrypted using algorithm like AES,DES and triple DES ,it generated public key are send to user personal mailed and then encrypted data again encrypted using system generated key after the encryption process completed then perform the decryption. Proposed system we realize a double attribute based encryption schema, what time only user one-to-many encryption method, and then user again encrypted the data after that double decryption where only users having the proper attributes and original system generated password only can decrypt their original message that are received from the network .For performing the decryption system generated based key are given and then the again it was decrypted using the key are generated from AES,DES ,triple DES .Similar to this proposed Double encryption based scheme performs and each and every time user selects someone of the algorithm AES ,DES and Tripe DES based on that performs the second encryption with system generated key only allowed to saw the login user or authentication user. This protection system uses some algorithms to charge data into unreadable text into two times which can be only being decoded or decrypted by party individuals possesses the associated key and their own system generated key also. Investigational results estimate the whole performance of the scheme with time; it indicates the proposed double encryption and decryption system providing more safety than the obtainable distributed authentication schema.

1. Introduction

MANETS are a great deal more susceptible to attacks than wired networks since of the remove average, active network topology, co-operative algorithms and require of centralized monitoring and management. In addition near these troubles, MANET nodes have incomplete series power and bandwidth. Safety basics direct us to have a layered safety measures approach to generate a protected network. The primary line of defense is perform usually by authentication and encryption schemes Ad hoc network consists of mobile nodes which converse with each additional through wireless medium with no any fixed communications. MANET consists of wireless nodes that progress with dynamism with no any boundary restriction. Mobile ad hoc network are additional level to safety threats and attacks.

Nodes in the network are able to common sense and find out nearby nodes [1]. They converse with every other by forwarding packets hop by hop in the set of connections [2]. As well the topology of the ad hoc network is animatedly changing and the nodes of the ad hoc network are frequently mobile. A major dispute in the design of the mobile ad hoc network is to keep its susceptibility from security attacks. As a lot of distributed systems, safety in ad hoc networks is based on the make use of a key management scheme for authentication. Definite key management systems contain to be developed to suit the individuality of mobile ad hoc networks [3].

For secure message over public network information can be protected by the method of encryption. Encryption convert that data into any unreadable text byte format, simply user having access to the key be able to decrypt the encrypted data. Encryption is a primary tool for the defense of responsive information. The reason to use encryption is confidentiality (prevent disclosure of information or privacy) in communications. Encryption is a method of talking to an important person whereas further people are listening, but such the other people cannot appreciate what you are seen. Encryption algorithms take part in a very important job in provided that information security alongside malicious attacks. In mobile devices safety is very significant and different types of algorithms are second-hand to thwart malicious attack on the transmitted data .Encryption algorithm can be categorize into symmetric key (private) and asymmetric (Public) key [6].

In MANET networks the Key organization is the major problem in ad hoc network as the nodes shift without restraint in the network and contain less memory. Symmetric key schemes use the ordinary key for both encryption and decryption. This method is earlier and easier to implement, and it lowers transparency on system assets. This type of safety mechanisms lack in data authentication and reliability. Public key cryptography use two keys that is public key and private key to create protected communication, in which the sender and receiver doesn’t necessitate sharing a secret key. These security methods (RSA) ensure data authentication and privacy not including shared secrets. Public key encryption is based on arithmetical function, computationally exhaustive and is not very well-organized for small devices in the network [4, 5].

In this paper we propose a new authentication schema in MANET against trust and network based model [7] .The network model is based on clustering models [8] in mobile ad hoc networks, propose a new method to perform authentication. Earlier than the formation of network model moreover we perform double encryption attribute based schema to make more security in the system using DES, AES, Triple DES. In this system when the user receives the message at each node based on double encryption first the original message was encrypted using anyone of the user selected algorithm AES, DES and Triple DES, then again it was encrypted using system generated key for login user .Because the general encryption schema not perform well in all data from this point the proposed double encryption and decryption achieves the best security than the normal trust model work with RSA,DES based methods ,scalable and distributed authentication service in the ad hoc networks.

The remainder of this paper is prepared in the following method: In section 2 discuss concerning the related work of various key management system and previous of the authentication model. Sections 3 describe the fundamentals of trust model and detail examination of proposed key authentication schema with additionally encryption schema. In Section 4, double attribute based encryption and decryption is evaluated with key size and the results are presented in Section 4. Finally, conclude the paper in Section 5.

2. Related Work

RSA Algorithm was developed by Rivest, Shamir and Adelman. RSA is a usually adopted public key cryptography algorithm. The main and silent the majority usually used asymmetric algorithm. RSA these days is used in hundreds of software products and can be used for key replace or encryption of tiny blocks of data. RSA use a variable size encryption block and a variable size key. Elliptic curve cryptographic scheme are public key mechanism so as to give the similar functionality as RSA schemes. ECC and RSA were introduced by Ranbir Soram and MemetaKhomdram [9]. Conversely, the safety of ECC is based on the rigidity of a dissimilar problem, which is the elliptic curve discrete logarithm problem (ECDLP). At present the best algorithms known to solve the ECDLP have fully exponential running time, in dissimilarity to the sub exponential-time algorithms recognized for the integer factorization problem. This means that a preferred security level can be attain with considerably smaller keys in elliptic curve systems than is probable with their RSA counterpart. The compensation that can be gain from smaller key sizes includes velocity and well-organized use of computing authority, bandwidth, and storage. It estimates of parameter sizes given that corresponding levels of safety for RSA and ECC systems. These comparisons demonstrate the application of elliptic curve cryptography particularly with high security.

J. Li, R. Li and J. Kato [10] classify the trust management model as repute-based structure and trust organization framework. A repute based structure uses direct surveillance and second-hand information distributed amongst a network to appraise other nodes. A trust organization structure evaluate neighboring nodes based on straight explanation while trust relationships between two nodes with no prior direct connections are built all the way through a grouping of opinion from middle nodes.

Marti et al. [11] proposed mitigating routing misbehavior by detecting non-forwarding nodes and rating every path so that those nodes are avoided when the routes remain recalculated. The follow-on behavior is present there that non-routing nodes are not included in routing paths for non-cooperation but they still can ask others to forward their messages. This scheme detects the misbehavior but it does not isolate it. Therefore, in our system, we are considering only those nodes which are isolated by rating their trust value as low as 0 for noncooperation.

Edith et al [12] discuss a trust model and a network model in arrange to improve the safety of open key certification. Their web model is constructed upon classified association or Clustering of the system by some Cluster to get better the safety and the competence of the network. It is second-hand based upon the web-of-trust mode with PGP.

In PGP, any user is able to act as the certifying authority. They describe trust quantitatively as a permanent value between 0 and 1. Here, the authors did not argue a mechanism for regeneration and revocation of the certificates. Conventional network authentication solution relies on physically there called certificate authorities (CAs). Safety supplies for CAs are significant with an examination of a broad variety of attacks so as to can be mounted against CAs [13].Well-liked network verification architectures comprise X.509 standard [14]. Though ad hoc linkages are located less-infrastructure, and there is no central server for key managements. Hence conventional CA-based solutions do not get together the necessities of the mobile ad hoc networks.

3. Trust And Clustering-Based Authentication With Double Attribute Based Encryption And Decryption Schema

The trust model and a network model in arrange to supplement the safety of public key certification. Their network model demonstration is based in the lead of hierarchical social order or clustering of the network by various clustering algorithms. The person behind perceives with the principle of get better the safety and the competence of the network. They consider that the networks have been separated into clusters with unique ids. Their trust model is based in the lead of the web-of-trust model comparable to PGP in which any user can act as the certifying authority. They explain trust quantitatively as a steady value between 0 and 1. Each node maintains a catalog of trust principles for other nodes in the network. A direct trust is specific as a trust link among two nodes in the same group, and a proposition trust as the trust association among nodes of dissimilar groups. In order to build the trust relationship, they consider that the nodes are prepared with a number of detecting constituent such as watchdog for monitoring the behavior of nodes.

Then the public key management system is contained within a cluster. Each and every time the corresponding node requests to validate a node in one more cluster, it communicates with many nodes in that cluster. It sort the set up nodes based on their trust level standards and compute a weighted trust value by merge its trust values of the introduce nodes to the object node. The last trust value is then stored and uses to assess other nodes in that group. Major benefit of the system is to establish and separate a high fraction of malicious nodes whereas comparing the results to PGP based methods. The difficulty is that the storage level of the trust values and their calculation is both memory and time overriding task. Furthermore the mobility of nodes leads to alter of membership of nodes in a variety of clusters. Refer [7] paper the details algorithm steps are presented .Before the secure communication can be performed we proposed a encryption and decryption to provide more security in a system, by performing single encryption becomes less so we perform a double encryption using the AES, DES and Triple DES.

3.1 Cryptographic Algorithms

For secure communication over public network data can be confined by the method of encryption. Encryption converts that information with the assist of encryption algorithm by means of the key. Basically user has access to the key can decrypt the encrypted data. Encryption is a primary instrument for the defense of sensitive information. The standard to use encryption is privacy that prevents revelation of information or confidentiality in communications. In mobile devices protection is very imperative and dissimilar types of algorithms are used to prevent malicious attack on the transmitted data. After that competition of all the encryption method based on every attributes selected by user is performed then again the encrypted attribute was encrypted using the system generated key .For example if the attribute is encrypted first time using anyone of the encryption algorithm selected by user, make more security again the system generated key is used to encrypt the attribute ,then decryption also performed in two times .The system generated key only stored in database and login user only allowed to saw the details it results more secure than the single encryption schema.

3.1.1 AES Algorithm

To afford more security AES uses types of transformation such as replacement permutation, mixing and key adding each round of AES except the last uses the four transformations .AES is a specification for the encryption of electronic data. It has been adopt by the U.S. government and now it is used as worldwide. AES is a symmetric-key algorithm, meaning the similar key is used for both encrypting and decrypting the data. AES was announced by National Institute of Standards and Technology (NIST). Originally called Rijndael, the cipher was developed by two Belgian cryptographers, Joan Daemen and Vincent Rijmen, and submits by them to the AES selection procedure. The name Rijndael is a play on the names of the two inventors. AES is based on a design principle known as a substitution-permutation network. It is fast in both software and hardware.

Generally AES uses 10, 12 or 14 rounds to process the corresponding key size are 128,192 or 256 bits depends on the each rounds Each round in AES takes several stages with a fixed block size of 128 bits and a key size of 128, 192, or 256 bits, while Rijndael can be individual with block and key sizes in any multiple of 32 bits, with a smallest of 128 bits. The block size has a concentrated of 256 bits, but then again the key size has no theoretical maximum. AES operates on a 4×4 column-major order matrix of bytes. Most AES calculations are done in a special limited field. The AES encryption is specified as a numeral of repetition of transformation rounds that convert the input plaintext into the final output of cipher text. Each round consists of numerous processing steps, together with encryption key. A set of reverse rounds are useful to transform cipher text back into the original plaintext using the same encryption key.

1. Key expansion round keys exist derived from the encryption key using Rijndael's key schedule.
2. Initial round
   - Add round key every byte of the state-run is combined with the round key by using bitwise XOR.
3. Rounds
   - Subbytes a non-linear replacement step any where every byte is replaced with another permitting to a lookup table.
   - Shiftrows a transposition step every where every single row of the state is moved cyclically a certain number of steps.
   - Mixcolumns a mingling operation which activates on the columns of the state, combining the four bytes in each column.
4. Addroundkey
5. Final Round (no mixcolumns)
   - Subbytes
   - Shiftrows
   - Addroundkey

3.1.2 Data Encryption Standard (DES) algorithm

The Data Encryption Standard (DES) is a before predominant algorithm for the encryption of electronic data. It was extremely influential in the progression of current cryptography in the educational world. Developed in the early 1970s at IBM and base on an earlier design by Horst Feistel algorithm was present to the National Bureau of Standards (NBS) subsequent the agency's enticement to proposition a candidate for the fortification of responsive unspecified electronic government data. The publication of an NSA-approved encryption standard concurrently resulted in its quick worldwide acceptance and extensive academic scrutiny. Controversy arise out of classified plan fundamentals, a comparatively short key length of the symmetric-key block cipher design, and the participation of the NSA, beneficial doubts about a backdoor. The strong academic inspection the algorithm conventional over time led to the contemporary sympathetic of block ciphers and their cryptanalysis.DES is the conventional block cipher an algorithm that takings a fixed-length string of plaintext bits as well converts it through a series of difficult operations into another cipher text bit string of the equivalent length. Now the case of DES, the block size is 64 bits. DES as well usages a key to customize the transformation, so that decryption can theoretically only be implemented by those who know the actual key used to encrypt. The key apparently be made up of 64 bits .however, simply 56 of these be situated actually used by the algorithm. Eight bits are used exclusively checking for parity, and are after that discarded. The in effect key length is 56 bits, and that one is always estimated as such. The key is nominally put in storage or passes on as 8 bytes, apiece with odd parity. The algorithm's generally configuration is exposed in Figure 1. Present are 16 indistinguishable stages of processing, termed rounds. Present is also an initial permutation (IP) and final permutation (FP). Previous to the major rounds, the building block is separated addicted to two 32-bit halve and process alternately .This type of the system is called as Feistel scheme. It reduces the greatly the task of chiefly in hardware, as present is no require for divide encryption and decryption algorithms. The ⊕ representations denote the exclusive-OR (XOR) operation. The F-function scramble half a block jointly with a number of the key. The production beginning the F-function is then joint with the additional half of the block, and the halves are swap earlier than the after that round. After the final surrounding the halves are swap; this is a characteristic of the Feistel organization which makes encryption and decryption comparable process.

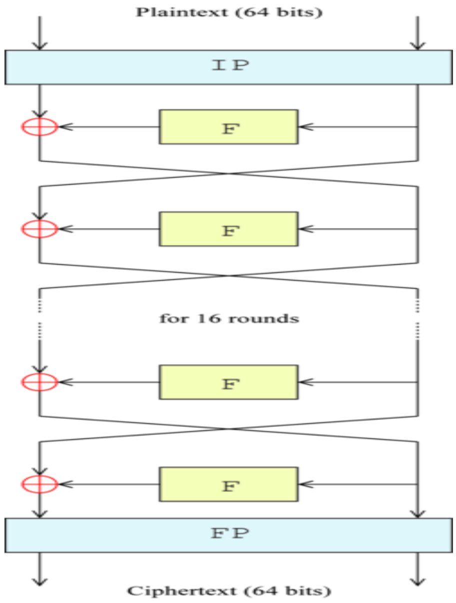

Figure 1: Structure Of the steps

The Algorithm of the DES -The Feistel function of DES

1. Expansion the 32-bit half-block is extended to 48 bits by means of the expansion permutation, denote E in the figure by duplicate half of the bits. The production consists of 48 bits pieces, each containing a copy of 4 equivalent input bits, plus a copy of the right away adjacent bit from each of the input pieces to either side.
2. Key mixing the effect is shared with a subkey with an XOR operation.16 48-bit subkeys single for each round are resulting from the main key by means of the key schedule
3. Substitution following combination in the subkey, the building block is separated into eight 6-bit pieces ahead of giving out by the S-boxes, or substitution boxes. Every one of the eight S-boxes replace its six contribution bits with four output bits according to a non-linear transformation, provide in the form of a lookup table. The S-boxes make available the core of the safety of DES with no them, the cipher would be linear, and unimportantly fragile
4. Permutation lastly the 32 outputs from the S-boxes are rearranged according to a FP, the P-box. This is calculated consequently with the intention of following permutation, each S-box's output bits are extend across 6 dissimilar S boxes in the next round. The F-function, depicted in Figure 2, operate on half a block (32 bits) at a point in time and consists of four stages is defined in algorithm steps.

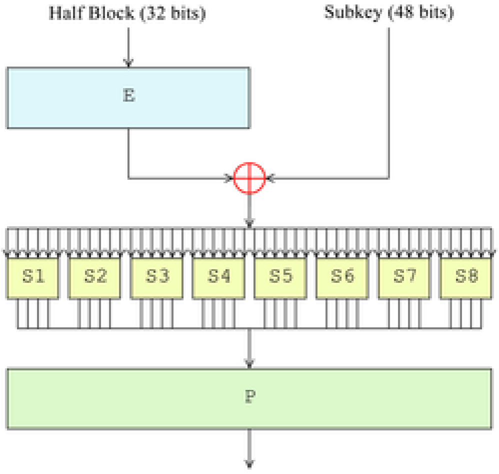

Figure 2: The Feistel function (F-function) of DES

3.1.3 Triple DES

In general DES algorithm are make less security than the system because brute force attack may be probable to occur a chance in the DES .To avoid these types of attack and make more security proposed a Triple DES algorithm that says concerning safety and the comparatively slow process of DES in to suggest a diversity of substitute block cipher designs, Most of these design reserved the 64-bit block size of DES, and might do something as a drop by substitute, even though they characteristically second-hand a 64-bit or 128-bit key.

DES itself can be modified and reuse in an additional secure scheme. Numerous previous DES user at the present use Triple DES (TDES) which be describe and analyses by single of DES's patentees (FIPS local 46-3); it involve apply DES three period by means of two or three DES with different keys. TDES is regard as sufficiently protected even though it is quite measured .A fewer computationally luxurious substitute is DES-X, which increase the key size by XORing extra key fabric previous to plus following DES. It is the way to rapidity up encryption, but it was exposed to be vulnerable to degree of difference cryptanalysis.

4. Results And Discussion

In this section we measure the performance of the proposed system that is AES, DES ,triple DES encryption and decryption schema. Performance of the system varies the times (ms) based on the key size specified by user. In the figure 1 shows that the performance of the system with four different methods and their corresponding time taken (ms) for both encryption and decryption results and double encryption and decryption methods based on AES,DES and Triple DES are measured .

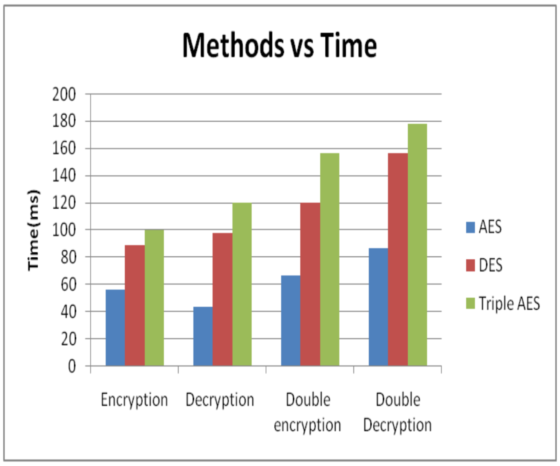

Figure 1: Algorithm vs. time

5. Conclusion

The accessible trust model that allow nodes to observe and rate every one with quantitative trust values. Defines the network model as clustering based, such that nodes take compensation of the neighboring monitor power and short communiqué distances to their collection members. In this work we additionally develop a double attribute based encryption and decryption schema with AES, DES and TDES using single encryption and second encryption was performed using System generated key for each and login user at the time of process, for exchange the data packets from one cluster of the nodes into another collection of the nodes in the clustered result. It involves a new certification effect than the obtainable trust based models keep posted their results on the lying users. In adding together calculate we manner the assessment results of double attribute based encryption and decryption schema with dissimilar key authentication to examine their performance and individuality in providing network security. Experimental results ensures that the security and public key authentication in the intrinsically unconfident and untrustworthy mobile ad hoc networks.

In this system the messages passed through cluster head may overload, creating a bottleneck due to additional message exchanges. To overcome these problem future directions may be the data aggregation based schema is performed in every user or each node in networks.

Reference

[1] C. Elliott and B. Heile, “Self-Organizing, Self-Healing Wireless Networks,” Proceedings 2000 IEEE Aerospace Conference, vol. 1, pp. 149–156, 2000.

[2] J. Broch, D. A. Maltz, D. B. Johnson, Y. C. Hu, and J. Jetcheva, “A Performance Comparison of Multi-Hop Wireless Ad Hoc Network Routing Protocols,” The 4th Annual International Conference on Mobile Computing and Networking (MobiCom’98), pp. 85-97, 1998.

[3] V. Karpijoki, “Security in Ad Hoc Networks,” Helsinki University of Technology, Tik-110.501 Seminar on Network Security, Telecommunications Software and Multimedia Laboratory, 2000.

[4]P.Ruangchaijat upon, P.Krishnamurthy, “Encryption and power consumption in wireless LANs-n,”The third IEEE workshop on wireless LANs ,pp 148-152 ,Newton Sep 27 , 28 2001.

[5]Hardjono, security in wirleless LANS and MANS , Artech house publisher,2005.

[6] Mohly Mohammad Hadhoud , “Evaluation the problem of Symmetric Encryption algorithms”, International journal of network security vol.10 May 2010.

[7]V.Gowthami, R. Buvaneswarim” An Efficient Attribute Based Schema for Trust and Cluster Based Authentication Mechanism in MANET”, International Journal of Advances in Computer Science and Technology, Volume 2, No.6, pp-77-82 ,June 2013.

[8]. Y. P. Chen and A. L. Liestman. A Zonal Algorithm for Clustering Ad Hoc Networks, International Journal of Foundations of Computer Science, vol. 14, pp. 305-322, 2003.

[9]Ranbir Soramand Memeta Khomdram,” Juxtaposition of RSA and Elliptic Curve Cryptosystem”, IJCSNS International Journal of Computer Science and Network Security, VOL.9 No.9, pp-11-20,September 2009 .

[10] .J. Li, R. Li and J. Kato, Future Trust Management Framework for Mobile Ad Hoc Networks: Security in Mobile Ad Hoc Networks, IEEE Communications Magazine, vol. 46, no. 4, Apr. 2008, pp. 108-114.

[11] S. Marti, T.J. Giuli, K. Lai, and M. Baker .Mitigating Routing Misbehavior in Mobile Ad Hoc Networks. Mobicom 2000, August 2000, pp. 255-265.

[12] C. H. Ngai Edith and R. Lyu Michael. Trust- and Clustering- Based Authentication Services in Mobile Ad Hoc Networks, 24th International Conference on Distributed Computing Systems Workshops - W4: MDC (ICDCSW’04), Hachioji, Tokyo, Japan, 2004. Vol 3/23-24.

[13] S. Kent, “Evaluating Certification Authority Security,” Proceedings 1998 IEEE Aerospace Conference, vol. 4, pp.319-327, 1998.

[14] PKIX Working Group, “Internet X.509 Public Key Infrastructure,” draft-ietf-pkix- roadmap-06.txt, 2002.

[15]. L. Zhou and Z. Haas. “Securing Ad Hoc Networks”, Consumer Communications and Networking Conference, 3rd IEEE, 10 – 14, 8-10 Jan. 2006.