ISSN 2320 - 2602

Volume 2, No.6, June 2013
International Journal of Advances in Computer Science and Technology
Available Online at http://warse.org/pdfs/2013/ijacst02262013.pdf

An Efficient Attribute Based Schema for Trust and Cluster Based 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,
gowthamishalini@gmail.com
[2]Head of Department IT & CT,
Hindusthan College of Arts and Science,
Behind Nava India, Coimbatore-641 028, Tamil Nadu, India,
buvana_ss@rediffmail.com

ABSTRACT

A mobile adhoc network is wireless communication network that have been collection of nodes with no fixed infrastructure and are able to discover the nearby node with lack of centralized control .Due to this lack of security issues occurs, so protecting the data or node in the network is essential in MANET. In recent works distributed system are mostly depend on key distribution and management system to make security. In this paper aims at providing the more secure and distributed authentication service. In existing system propose a secure public key authentication service based on a trust model and a network model to prevent nodes from obtaining false public keys of the others when there are malicious nodes in the networks. Using the public key authentication model, it is important to reduce the key distribution complexity in MANET. Proposed system we implement an attribute based encryption schema, when only user one-to-many encryption method, where only users having the proper attributes can decrypt their original message that are received from the network . Because the Security of information have been become an important issue in MANET. Here the Encryption has been become a solution and plays important role in information security system. This protection mechanism uses some algorithms to rush data into unreadable text which can be only being decoded or decrypted by party those possesses the associated key. Corresponding encryption methods are RSA, AES with each of them having own private and public key. Experimental results evaluate the overall performance of the system with time; it indicates the proposed system providing more security than the existing distributed authentication schema.

Key words: MANET, Trust, Clustering, Authentication, encryption and decryption schema.

1. INTRODUCTION

Mobile Ad Hoc Networks (MANETs) have been received significantly increasing interest, partially owing to the potential applicability of MANETs to numerous applications. The employment of such networks, poses numerous challenging issues due to the self-motivated nature of the nodes with arbitrary topology and transmission errors with the limited wireless range of nodes. Since all the nodes in the network collaborate to forward the data, the wireless channel is flat to active and passive attacks by malicious nodes, such as Denial of Service (DoS), eavesdropping, spoofing, etc. Implementing security is therefore of prime importance in such networks.

The five components of a security mechanism are confidentiality, authenticity, availability non-repudiability and integrity, from all of these the authenticity is the most fundamental issue. One of the widely used authentication mechanisms in conventional wired networks is the public key management system using certificate based schema.

A mobile ad hoc network is a collection of nodes with no infrastructure while its nodes are connected with wireless links. Nodes in the network are capable to sense and determine nearby nodes [1]. They communicate with each other by forwarding packets hop by hop in the network [5]. Also, the topology of the ad hoc network is dynamically changing and the nodes of the ad hoc network are often mobile. The major issue in the design of mobile ad hoc network is

to protect its vulnerability from security attacks. A lot of distributed systems, security in MANET are based on the use of a key management system for authentication and key certificate based authentication mechanism. Specific key management systems have to be developed to suit the characteristics of mobile ad hoc networks [6].

Overcome the issues of designing the MANET and protect the network against the attacks, in this paper first we proposed a new key management scheme with a well-defined trust model and a network model. Proposed trust model follows the "web of trust" approach proposed in Pretty Good Privacy [7] with numerous ways. The network model is based on clustering models [8] in mobile ad hoc networks, propose a new mechanism to perform authentication. Before that the creation of network model additionally we perform two encryption schemas to make more security than the system such as RSA, DES. When the user receives the message at each node based on attribute based encryption schema, here we randomly change the any encryption schema at each and every time of the node selection. The proposed system achieving the higher security than the normal trust model, scalable and distributed authentication service in the ad hoc networks.

The remainder of this paper is organized in the following manner: In section 2 discusses about the related work of various key management system and earlier of the authentication model. Section 3 define the basics of trust model and detail analysis of proposed key authentication schema with attribute based encryption schema .In Section 4, proposed system is evaluated with key size and the results are presented inSection 4. Finally, conclude the paper in Section 5.

2. RELATED WORK AND SURVEY

Certificate-based authentication usually consists of three phases. During the primary phase, the nodes are issued a certificate by a certifying authority. The certificate is formed by the CA using the node's identity information such as IP address, organization and its public key. The certificate also consists of the issuing time and the expiration time besides other information. During the following phase the certificate is "renewed" due to its expiration. The final phase involves revocation of the certificate by the CA, probably due to cooperation of the private key of the certificate holder, or possibly because the issuer believes that the user-key binding is no longer valid.

One of the certificate-based authentication methods proposed by Capkun with the formation of certificate graphs [9]. The suggested approach is similar to PGP certificates [2], apart from the fact that in PGP a central certificate server is used. Capkun et al argue that the use of two repositories is in providing a good estimate of the certificate graph and for node authentication. Capkun et al propose algorithms such as Maximum degree algorithm based on finding the path in the certificate graph with highest number of certificates.

Capkun et al do not mention any explicit certificate renewal process as it is done whenever a node finds expired certificates in its non-updated certificate repository. They recommend two methods, one explicit and the other implicit, for revocation of the certificates. However the drawbacks of this system are the exclusive tables that comprise to be maintained for the certificate repositories and every time a node moves from one region to another, it has to renegotiate with other nodes and modernize the tables again.

Kong et al [3] propose a distributed certification based on threshold cryptography and shared secrets. The necessary goal of a threshold secret sharing method is to share a secret key k among an arbitrarily large community using a secret polynomial f(x). If the degree of f(x) is (k-1), any k members of the community can recover the secret key, whereas any members a lesser amount of than k reveals no information of the secret [10]. Based on this, a node receives its public key from its k neighboring nodes. Here, k is a parameter which requests to be carefully tuned so that the method it is more effective.

Wang, Zhu and Li [4] propose a novel mechanism in which CAs from different administrative domains can co-exist in the network. They moreover suggest a distributed certificate authority by using k-threshold secret sharing similar to the method introduced by Kong et al [3]. In this method if the two nodes don't have a regular CA, then they progress to investigate their one-hop and two-hop neighbors through a Distributed Multi-hop Certificate Request (DMCR) algorithm. The steps for certificate renewal are similar to the DMCR scheme. But the certificate revocation is not discussed in this method.

Pretty Good Privacy (PGP) [7] is proposed by subsequent of a web-of-trust authentication model. PGP uses digital signatures as its creates the structure for introduction. When any user signs for any more user's key, he or she become an introducer of that key. As this process goes on, a web of trust is

established. Nevertheless, the distribution of certificates is based on publicly accessible certificate directories that reside on centrally managed servers, which is not a fully self-organized approach.

Zhou and Hass [10] proposes a partially-distributed certificate authority that makes use of a (k,n) threshold scheme in distributing the services of the certificate authority to a set of specialized server nodes. However, high mobility causes frequent route changes, thus contacting the local CA in a timely fashion is non-trivial. Besides, in ad-hoc networks, the local CA may be multi-hops away and also move. This not only cause problematical dynamic repartitioning of the network, but also stretches the problem of locating and tracking a local CA server. Moreover, every local CA is exposed to single point of compromises or denial of service (DoS) attacks. Comparable public key infrastructure service called MOCA (Mobile Certificate Authority) also employs threshold cryptography to distribute the CA functionality over specially selected nodes based on the security and the physical characteristics.

3. TRUST AND CLUSTERING-BASED AUTHENTICATION

The trust model and a network model in order to augment the security of public key certification. Their network model representation is based in the lead of hierarchical society or clustering of the network by various clustering algorithms. The author perceives with the purpose of improve the security and the efficiency of the network. They believe that the network have been divided into clusters with unique IDs. Their trust model is based upon the web-of-trust model similar to PGP in which any user can act as the certifying authority. They describe trust quantitatively as a constant value between 0 and 1. Every node maintains a list of trust values for other nodes in the network. A direct trust is definite as a trust relationship between two nodes in the same group, and a suggestion trust as the trust relationship between nodes of different groups. In order to construct the trust relationship, they believe that the nodes are equipped with some detecting component such as watchdog for monitoring the behavior of nodes.

Public key management is implicit to be present within a cluster. Every time a node requests to authenticate a node in one more cluster, it communicates with numerous nodes in that cluster. It sorts the introduce nodes based on their trust level values and computes a weighted trust value by combine its trust values of the introducing nodes to the target node. The finishing trust value is then stored and used to evaluate other nodes in that group. Main advantage of the system is to determine and segregate a high percentage of malicious nodes while comparing the results to PGP based methods. The disadvantage is that the storage space of the trust values and their computation is both memory and time consuming. Additionally the mobility of nodes leads to change of membership of nodes in various clusters.

The following algorithm shows the operation of s in obtaining the public key certificates of the t .To request the public key of t, *s* first looks up the group ID φ_t.Of node *t*. Then, it sorts the trust values of nodes that belong to and selects the nodes with the highest trust values as introducer's i_1, i_2 …, i_n, and sends them request messages. After collecting the reply messages that are encrypted by introducers' secret keys, *s* decrypts the messages with the corresponding public keys. Next, it compares the public keys obtained from the reply messages and selects Pk_t as the one with majority votes. If there is no majority vote, *s* tries to select more introducers and sends the request messages again when it is possible. After that, it reduce the trust ideals of the nodes which do not agree with that public key, so to avoid selecting these nodes, now deemed dishonest or malicious, as introducers in the future. Finally, *s* calculates and updates the trust value of *t*, V_t.

1. Looks up the group ID of *t*, φ_t.
2. Sorts the trust values of nodes belonging to group φ_t in the trust table. Let i_1, i_2,…, i_n where denote nodes with the highest trust values in group .
3. Sends request messages to nodes in *I*.
4. Collects the reply messages *from*i_1, i_2… i_n, where $m = \{Pk_t, V_{ik,t}\}_{SK_{ik}} Pk_t$denotes the public key of node *t*, $V_{ik\ ,t}$ denotes the trust value from $i_k$to *t*, and SK_{ik}denotes the secret key of i_k. The reply message is signed by the secret key of i_k, Sk_{ik}.
5. Compares the public keys received and selects Pk_t with the majority votes. Let $i_{good} \in I_{good}$ and $I_{bad} \in I_{bad}$ where i_{good} are the nodes that thought to be honest (agree on $Pk_t$with the majority) and i_{bad} are the remaining nodes considered dishonest.
6. Reduces the trust values of i_{bad} to zero. Computes and updates the trust value of *t*, V_t, with the following formulae: $V_{S,ik,t} = V_{s,ik}\theta V_{ik,t} = 1 - (1 - V_{ik,t})^{V_{s,ik}}$and $V_t = 1 - \prod_{k=1}^{n}(1 - V_{s,ik,t})$where $i_k$denote the nodes in $I_{good}$and *n* denotes the number of nodes in I_{good}.

3.1 Cryptographic Algorithms

For secure communication over public network data can be protected by the method of encryption. Encryption converts that information with the help of encryption algorithm using the key. Simply user having access to the key can decrypt the encrypted data [11]. Encryption is a fundamental tool for the protection of sensitive information. The principle to use encryption is privacy that preventing disclosure of information or confidentiality in communications.

Encryption is a manner of talking to somebody whereas the other people are listening, however such the other people cannot understand what you are saying [11].

Encryption algorithms play a vital role in providing data security against malicious attacks. In mobile devices protection is very imperative and dissimilar types of algorithms are used to prevent malicious attack on the transmitted data.

Encryption algorithm can be categorized into symmetric key (private) and asymmetric (Public) key [12]. In Symmetric keys encryption or secret key encryption, simply one key is used to encrypt and decrypt data. In Asymmetric Keys generally two keys are used i.e. is private and public keys. Public key is used for encryption and private key is used for decryption (e.g. RSA).

RSA Algorithm

RSA stands for Rivest, Shamir and Adleman. RSA is a commonly adopted public key cryptography algorithm. The primary and silent most commonly used asymmetric algorithm. RSA nowadays is used in hundreds of software products and can be used for key exchange, or encryption of tiny blocks of data. RSA uses a variable size encryption block and a variable size key. The key-pair (p,q) is derivative from a very large number n, that is the result of two prime numbers (p,q) are selected according to particular rules. RSA has been extensively used for establish secure communication channels and for authentication the identity of service provider over insecure communication medium.RSA involves a public key and a private key. The public key can be well-known to everybody and it is used for encrypting original messages from the communication. Messages encrypted with the public key can only be decrypted in a sensible amount of time using the private key.

The keys for the RSA algorithm are generated the following way:

1. Choose two distinct prime numbers p and q.
    - For security purposes, the integer's p and q should be chosen at random, and should be of similar bit-length. Prime integers can be efficiently found using a primarily test.
2. Compute n = pq. n is used as the modulus for both the public and private keys. Its length, usually expressed in bits, is the key length.
3. Compute $\varphi(n) = \varphi(p)\varphi(q) = (p - 1)(q - 1)$, where φ is Euler's totient function.
4. Choose an integer e such that $1 < e < \varphi(n)$ and $\gcd(e, \varphi(n)) = 1$; i.e. e and $\varphi(n)$ are coprime.
e is released as the public key exponent.
5. Determine d as $d-1 \equiv e \pmod{\varphi(n)}$, i.e., d is the multiplicative inverse of e (modulo $\varphi(n)$).
    - This is more clearly stated as solve for d given $de \equiv 1 \pmod{\varphi(n)}$
    - d is kept as the private key exponent.

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 [11].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 maximum of 256 bits, but 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 finite field. The AES cipher 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. KeyExpansion round keys are derived from the cipher key using Rijndael's key schedule.
2. InitialRound
    - AddRoundKey each byte of the state is combined with the round key using bitwise XOR.
3. Rounds
    - SubBytes a non-linear substitution step where each byte is replaced with another according to a lookup table.
    - ShiftRows a transposition step where each row of the state is shifted cyclically a certain number of steps.
    - MixColumns a mixing operation which operates on the columns of the state, combining the four bytes in each column.
4. AddRoundKey
5. Final Round (no MixColumns)
    - SubBytes
    - ShiftRows
    - AddRoundKey

4. EXPERIMENTAL RESULTS

In this section we measure the performance of the proposed system that is RSA, 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 key size values and their corresponding time taken (ms) for both RSA encryption and decryption results. Results values of figure 1 are tabulated at table 1 and shown in the below:

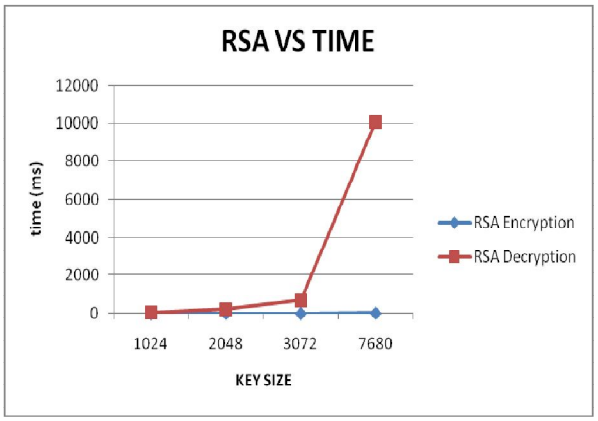

Figure 1: RSA algorithm vs. time

Table 1: RSA algorithm vs. time

KEY SIZE	***RSA ENCRYPTION***	***RSA DECRYPTION***
1024	03.04 ms	203.65 ms
2048	15.21 ms	31.51 ms
3072	31.96 ms	703.21 ms
7680	16.86 ms	10093.05 ms

Table 1: RSA algorithm vs. time

In the figure 2 shows that the performance of the system with four different key size values and their corresponding time taken (ms) for both AES encryption and decryption results. Results values of figure 2 are tabulated at table 1 and shown in the below

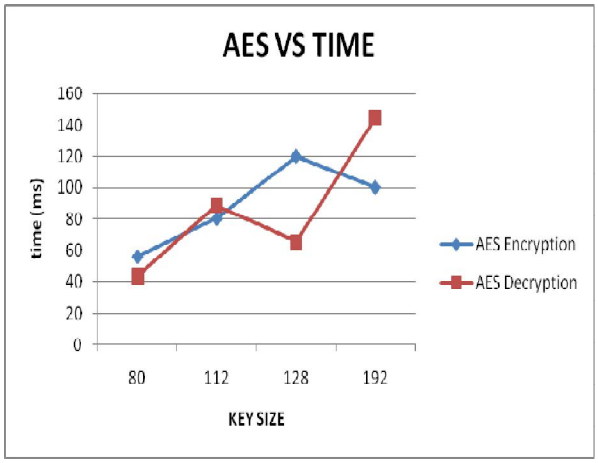

Figure 2: AES algorithm vs. time

Table 2: AES algorithm vs. time

KEY SIZE	***AES ENCRYPTION***	***AES DECRYPTION***
80	56ms	43.43ms
112	80 ms	89ms
128	120ms	65.5ms
192	100ms	145ms

Table 2: AES algorithm vs. time

5. CONCLUSION AND FUTURE WORK

The existing trust model that allows nodes to monitor and rate each other with quantitative trust values. We define the network model as clustering-based, such that nodes take advantages of the neighboring monitoring power and short communication distances

to their group members. In this work we additionally develop a RSA, AES schema for exchanging the data packets from one group of the nodes into another group of the nodes in the clustered result. It involves a new authentication result than the existing trust based models update their results on the dishonest users. In addition measure we conduct the evaluation results of two encryption and decryption schema with different key authentication to observe their performance and characteristics in providing network security. Our approach ensures the security and availability of public key authentication in the inherently insecure and unreliable mobile ad hoc networks.

In this system the messages passed through cluster head may overload, creating a bottleneck due to additional message exchanges. The issues of the security, flexible access, user revocation are the important challenges towards achieving the fine-grained, cryptographically forced data access control. Future work we make the consideration of system with fine grained and more efficient.

REFERENCES

2. P. Zimmerman. **The Official PGP Users guide**, *MIT Press*, ISBN 0-262-74017-6, 1995.

3. J. Kong, P. Zerfos, H. Luo, S. Lu, and L. Zhang. **Providing robust and Ubiquitous Security support for Mobile Ad Hoc Networks**, *Proceedings of the 9th International conference on Network Protocols (ICNP)*, Riverside, California, USA, November 11-14 2001.

4. Weihong Wang, Ying Zhu, Baochun Li. **Self-Managed Heterogeneous Certification in Mobile Ad Hoc Networks**, in *the Proceedings of IEEE Vehicular Technology Conference (VTC 2003)*, Orlando, Florida, 10/6-9, 2003.

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

5. 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.

6. V. Karpijoki. **Security in Ad Hoc Networks**, *Helsinki University of Technology*, Tik-110.501 Seminar on Network Security, Telecommunications Software and Multimedia Laboratory, 2000.

7. S.Garfinkel. **PGP: Pretty Good Privacy**, *O'Reilly & Associates Inc*., USA, 1995.

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. S. Capkun, L. Buttyan and J-P Hubaux. **Self-Organized Public-Key Management for Mobile Ad Hoc Networks**, *IEEE Transactions on Mobile Computing*, Vol. 2, No. 1, Jan-Mar 2003, pp. 52-64.

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

11. Marshall D. Abrams, Harold J. Podell on cryptography.

12. Mohly Mohamad Hadhoud. **Evaluation the problem of Symmetric Encryption algorithms**, *International journal of network security*, vol. 10, May 2010.

13. NeetuSettia. **Crypt analysis of modern cryptography Algorithms**, .*International Journal of Computer Science and Technology*, December 2010.