SECURE KEY GENERATION USING CRT IN MANET

Dr. K. Selvakumar[1], N.Seethalakshmi[2]
[1]Associate Professor, [2]Research Scholar
[1]Department of Information Technology, [2]Department of Computer Science and Engineering,
[1,2]Annamalai University

Abstract
Security is one in every of the main issues in Mobile Adhoc Networks as a result of existing routing protocols for wireless networks don't offer a secure communication. Key management is an essential part of multicast security. Mobile Adhoc Networks are dynamic and more prone to unauthorized action. A Key administration is essential piece of security. Key administration protocols at that point assume a key part in any safe group communication architecture. The key administration is an imperative challenge due to its dynamism that influences extensively its execution. In this paper, a new scheme is introduced named as CRT that is based on key management technique. The simulation results are compared with packet delivery ratio, throughput, delay and energy.
Keywords: MANET, Key Management, Chinese Remainder Theorem

1. INTRODUCTION

The point of a security benefit is to secure system before any assault happened and made it harder for a malicious node to breaks the security of the system. Because of extraordinary highlights of MANET, giving these administrations confronted heaps of difficulties. For securing MANET an exchange-off between these administrations must be given, which implies on the off chance that one administration ensures without seeing different administrations, security framework will fall flat. Giving an exchange off between these security administrations is replied upon organize application, yet the issue is to give benefits one by one in MANET and exhibiting an approach to ensure each administration as far as Availability, Authentication, Data Confidentiality, Integrity and Non-Repudiation. [1]

Security is one of the major issues in MANETs. Their natural characteristics make them vulnerable to passive and active attacks, in which misbehaving nodes can eavesdrop or delete packets, modify packet contents, or impersonate other nodes. It is widely acknowledged that public key cryptographic mechanisms can provide some of the strongest techniques against most vulnerability. These mechanisms use public/private key pairs to encrypt and decrypt messages. However, the use of traditional public key cryptography over MANETs can cause severe computational, memory, and energy overhead [2].

The proposed model will use a very lightweight non-predictive key exchange scheme with secure routing mechanism in order to protect the MANETs. The proposed scheme will be designed to overcome the shortcomings of the existing model. The proposed model will be using the multi-column random key table generation to improve the level of security and lower the overhead and transmission delay. The proposed scheme will use the secure periodic update to change the key table, which removes the need of encryption, hence will definitely lower the transmission delay due to the encryption or decryption algorithm [3].

2. RELATED WORK

This paper presents a secured ID-based key management scheme for MANETs which permits mobile nodes to derive their public keys directly from their known network identities and with some other common information. Most existing security mechanisms for MANETs thus far involve the heavy use of public key

certificates. Our solution obviates the need of any inline Certification Authority (PKI) to share secret key. It also provides end-to-end authentication and enables mobile user to ensure the authenticity of user of peer node. The significant advantage of our solution is to avoid users to generate their own public keys and to then distribute these keys throughout the network. This scheme solved the security problem in the ad hoc network and is also suitable for application to other wired and wireless network [4].

This paper presents IKM (ID-based key management), a secure, lightweight, scalable IKM scheme for MANETs. As a novel combination of ID-based and threshold cryptography, IKM is a certificateless solution that permits public keys of mobile nodes to be directly derivable from their known network IDs and some other common information. It thus obviates the need for public-key distribution and thus certificates inherent in conventional public-key solutions. Our IKM is characterized by a novel method of constructing IDbased public/private keys, which not only guarantees highlevel resilience to node compromise attacks but also facilitates very efficient network-wide key update by a single broadcast message. In addition, we give general guidelines on choosing the secret-sharing parameters for achieving desirable levels of security and robustness [5].

Securing message transmission normally involves some encryption at source node and decryption at destination node of messages using RSA technique which leads to a large computational overhead. Instead, we use combination of RSA and CRT schemes which reduces the computational overhead to a large extent. Also, the presence of the malicious nodes in the network is the cause of packet loss during transmission of messages through those nodes. Algorithm RSRP tries to identify the set of disjoint routes considered as probable routes between a source-destination pair which are free from those malicious nodes [6].

A new key-star-based key management protocol (key value = ‘n’ bit numbers) has been proposed in this paper. The proposed algorithm focuses mainly on the minimising KS and user’s computation complexity. When the key size is small (key size = 128 bits), the computation time decreases by around 700 ms in the KS area and when the key size increases (1024 bits) the computation time decreases by around 35 000 ms for updating a single key from the dynamic multicast group. With regard to the storage complexity, the amounts of keys stored by group members are almost same and a slight increase in KS storage space [7].

This paper presents a multiway tree based group key management scheme using CRT for multi-privileged group communications. The proposed scheme employs multiway trees to construct SG-subtrees in the key graph in order to reduce the height of key tree. The KDC in our scheme distributes encrypted rekeying materials instead of encrypted new keys, and compresses them into a smaller message by using CRT for the leaving and switching process. The proposed scheme will be unsuitable for a distributed environment, which cannot deploy a centralized manager with certain computing power and may not work well in the network with a high delay. Moreover, the proposed scheme cannot reconstruct the DG subgraph currently so that it does not support dynamic formation and composition of service groups [8].

In the proposed scheme the communicational cost is reduced by eliminating the re-keying processes and avoiding the tree balancing. To reduce the server computational cost the member’s private key is computed by individual members at their own site. The proposed scheme maintains the uniqueness of the prime factors contributing to the secret value X that helps in maintaining the forward and backward secrecy. The storage overhead is distributed among the members and the server to reduce the storage complexity. The message encryptions are performed by using the Square and multiply method to reduce the encryption cost. The decryption operation is based on the Chinese Remainder Theorem that speeds up the message decryption process [9].

We proposed an authenticated group key distribution protocol based on the CRT. Each user needs to register and obtain a secret from the KGC initially. In real-time operation, the KGC can broadcast a secret group key to all members based on all members’ secrets. The secret shared between each user and the KGC can be reused for multiple group communications. The

confidentiality of our proposed protocol is unconditionally secure [10].

3. Existing Key Management Scheme

In a troublesome key administration plot [11], the created key is passed utilizing number of distribution strategies. The entire system characteristic relies upon those methods. The Coding and Decoding (CODEC) utilizes a pair-wise key taking care of framework that limits the quantity of keys utilized to limit the key generation and distribution times. The basis limitations in key management schemes are

- Maximizing Security
- Maximizing mobility
- Limiting key handling time
- Limiting power

Multiple Key Management Scheme based Identity

This kind of key management scheme includes 4 phases as below.

3.1. Network Initialization

Network Initialization comprises of following process. They are

1. *Generation of pairing parameters and key Initiation:*

This process contains the system setup and also extraction of private key. The framework scheme taken for creating random keys in addition with public key generator that can be treated as PKG (). This PKG is taken to give pair of keys like public and private from client's id data.

2. *Generation of pair-wise keys:*

This process [12] is taken to produce pair-wise keys. It set up a link between sender and receiver using session keys. Session keys are taken to encode/decode the original data that guaranteeing the MANET as a secured communication.

3. *Verifiable secret sharing:*

This task comprises of 2 stages as follows

i. Sharing phase
ii. Reconstruction Phase.

In threshold phase, every one of the group heads take part at the same time to build the particular secret key. The encoded id is used as a subshare that is sent to group heads by taking the public key and be checked. Every time successfully checked the subshare, at that point it is confirmed that the value got from cluster head is right otherwise that cluster head is declared as compromised node and this node will be expelled from the database.

3.2. Key Revocation

This process comprises of three subtasks.

i. *Misbehavior Report:* If the network is recognizing that the group head is behave badly, that specific group head will be expelled from the list then remaining keys will be refreshed quickly.
ii. *Revocation Generation:* In this tasks, it is the group head removal process from the list. The Revocation Head will based upon its identity.
iii. *Revocation Verification:* If the overflow message by nodes from revocation head is gotten concerning the concession node, the insights concerning that identity of node will be expressed in its revocation key. Additionally by guaranteeing the node that no far interaction/ transformation which assist the network to accomplish safe transformation.

3.3. Multiple Secrets Key Update

The identity based multiple secrets key administration plan is refreshing the keys occasionally by refresh plan and furthermore the key refresh occurred on whatever occasion any nodes are recognized as concession node, promptly every nodes will get recent keys then only cryptanalyst can't respond or hold data.

3.4. Member Joining and Eviction

This process is taken to include new nodes as group heads to organize. The connecting plan is characterized in certain plan then the transformation price and computation cost as well will be lessened. Group head removal can be carried whenever, at whatever node's status becomes inaccessible status or node getting communication failure.

4. Proposed CRT- key management scheme

The key always ascertained in sets (CRT) influence the key computation time is diminished quite. This has a prompt impact in all other system parameters they portray the idea of the system. Let $N_1,N_2,\ldots\ldots N_t$ are set-wise generally prime positive whole numbers and let $a_1,a_2,\ldots\ldots a_t$ be integers. Then congruence's, $x \equiv a_j \pmod{m_j}$ for $1 \leq j \leq t$, has a special arrangement modulo $N= n_1 \times n_2 \times \ldots \times n_t$ which is given by

$$y \equiv a_1 N_1 x_1 + a_2 N_2 x_2 + \ldots\ldots + a_t N_t x_t \ (mod\ N) \qquad (1)$$

Where $N_i = N/n_i$
and $X_i \equiv (N_i) - 1\ (mod\ n_i)$ for $1 \leq i \leq t$.

5. Working principle of Proposed work

Every node in the system makes two keys for encryption and decryption of messages. Each node creates one public key and one private key. All the nodes in the system take the idea of Rivest Shamir Algorithm and also Chinese Remainder Theorem. All nodes similarly arrange another key for a kind in connection to public and private key. This key is called security key. This type of security key is taken to perceive the paths from source to destination where there are no malicious nodes.

The source node communicates to all other neighbors through RREQ data. The RREQ data is forward through neighbor node and this procedure continues till destination node is found. Goal node gets distinctive RREQ bundles from different paths and send back acknowledgement data through those paths to source node. Source node makes routing table that keeps all path data.

Secure-key (S) can be produced with the help of Chinese Remainder Theorem in source node. The secure-key is separated into n part using the source node. K-subset of n parts can be used to recreate the Secure-key. SN decides estimate of n on the premise of accessible paths to the goal. SN makes a expression F(x) with degree n and creates n value of focuses. It encodes every points using RSA with public key of destination node. These encoded n focuses are moved by source node to the goal node using n number of various paths. Goal node deciphers it with its private key using CRT (Chinese Remainder Theorem)and again resends each of these points in encoded form to source node with public key of source node through n number of different routes. Source node decodes all the encrypted points with private key of it using CRT. Presently source node using Lagrange's Interpolation Theorem revamps polynomial using k set of points from n set of points and decides constant without any coefficients (S1). If S1=S, these k points are substantial else they are invalid. This invalid set of k points is coming from k distinctive paths. One of these paths is not secure because to the presence of malicious nodes. Source node keeps away these k paths and acknowledges those k paths whose k points build valid set. Source node sends messages to the destination node through these protected k paths in encrypted form. Receiver decrypts this message using CRT. This way all messages are sent to the destination node safely.

5.1 Key Generation

In key generation process, two keys are used. One is public key and another one is private key. Normally the generation of keys in the following ways:

1) All node produces two prime values a,b.
2) M=ab.
3) Θ(H) = (a-1)(b-1).
4) Choose z such that z is not divisor of Θ (H) and 1 is less than z and z is less than Θ (H).

5.2 Encryption

The encoding of message from source to destination carried out using RSA in the following line:

$T=J^e \bmod H$

Where,
H= cipher text.
J=plain text
e,H=public key of destination node.

5.3 Decryption

The decoding of message in the destination using CRT in the following line:

$dp = d \bmod (p-1)$.
$dq = d \bmod (q-1)$.
$q_{inv} = q^{-1} \bmod p$.
$m_1 = C^{dp} \bmod p$.
$m_2 = C^{dq} \bmod q$.
$h = (q_{inv} * (m_1 - m_2)) \bmod p$.
$M = m_2 + h*q$

Where,
p,q= Two prime numbers such that N=p.q.
d,N=private key of destination node.

5.4 Secure key Generation

The source node(SN) produces secure key using CRT. Production of secure key is resolved following way:

1) SN creates number of integers $m_1, m_2, m_3, \ldots\ldots m_n$,such that greatest common divisor$(m_i, m_j)=1$.
2) $m= m_1.m_2.m_3.\text{-----}.m_n$.
3) $a_1, a_2, a_3, \ldots\ldots a_n$ be the pair of integers.
4) $T \equiv a_1 (\bmod m_1)$

$T \equiv a_2 (\text{mod } m_2)$

.

.

.

.

.

$T \equiv a_n (\text{mod } m_n)$

$T = a_1 y_1 T_1 + a_2 y_2 T_2 + \ldots\ldots\ldots + a_n y_n T_n$

$T_i = m/m_i$, $y_i = T_i\text{-}1 \ (\text{mod } m_i)$.

5) S=m.

6) S is the secure key of source node.

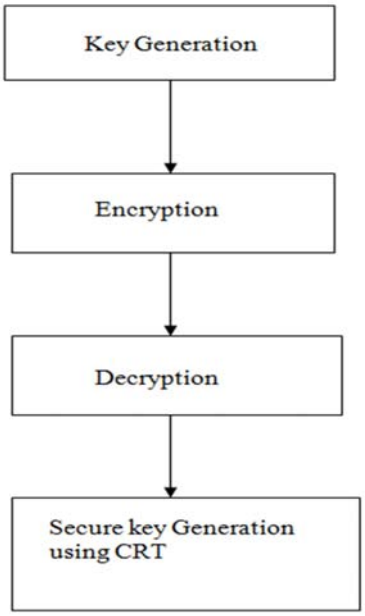

Fig 1: Block diagram of proposed work

6. PERFORMANCE EVALUATION

When number of nodes increases from 10 to 100, the performances of Secure Routing Scheme gives better results. When the number of nodes increases, the performance are shown below. Computational complexity of proposed Scheme is higher than proposed routing protocol. Proposed Scheme uses RSA modular expansion for decryption. CA-AOMDV protocol takes CRT for decryption whose computational complexity is lower than RSA modular expansion scheme.

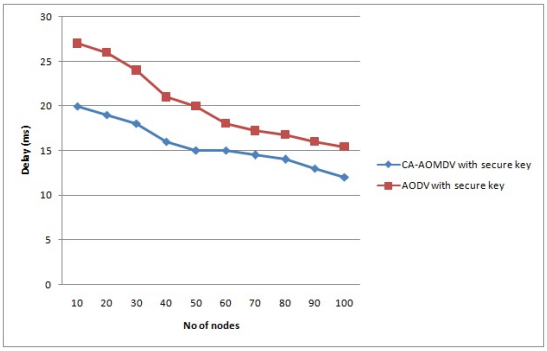

Fig 2. Variation of delay with number of nodes

From figure 2, it is clearly seen that our proposed method secure key in AODV give 80% result than existing system.

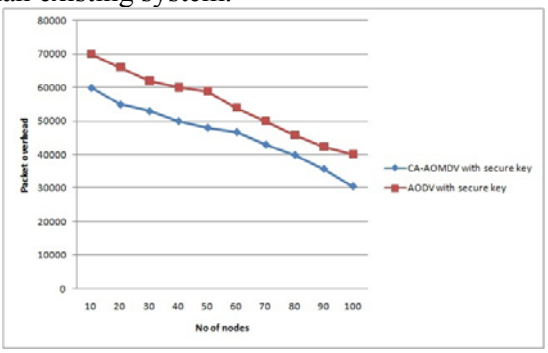

Fig 3. Variation of packet overhead with number of nodes

In figure 3, the packet overhead is 84% in our proposed work Secure key in AODV and maximum in existing work.

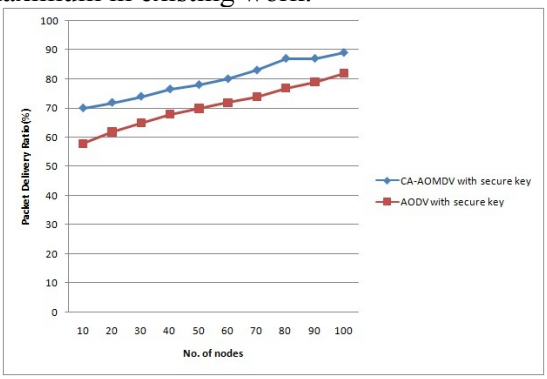

Fig 4. Variation of packet delivery ratio with number of nodes

In figure 4, it is shown that our work secure key in AODV gives 89% packet delivery ratio than existing system.

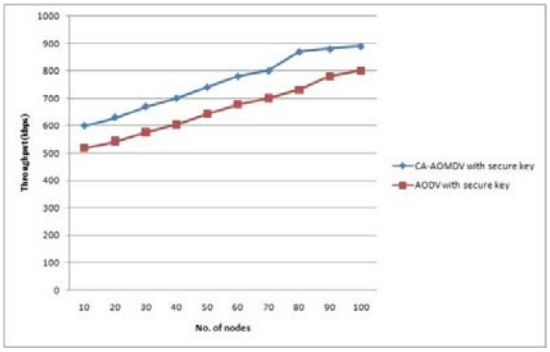

Fig 5. Variation of throughput with number of nodes

From figure 5, the throughput is 86% in our work than existing system.

7. CONCLUSION

Security is one of the major explores in MANET. A Key management is fundamental part of security. Key administration protocols then assume a key part in any protected group communication design. The key administration is a critical test due to its dynamism that influences significantly its execution. In this work, a new scheme is introduced using Chinese Remainder Theorem based key management technique compared with id based multiple key management. The RSA calculation expanded the overload of network. Here the CRT diminishes the encryption complexities. The simulation results demonstrate that execution of proposed protocol gives 85% outcome. The simulation results are enhanced in terms of packet delivery ratio, throughput, delay and energy.

REFERENCES

[1] Ali Dorri and Seyed Reza Kamel and Esmail kheyrkhah , "Security Challenges In Mobile Ad Hoc Networks: A Survey", International Journal of Computer Science & Engineering Survey, pp.15-29, 2015.

[2] Eduardo da Silva , Aldri L. dos Santos , Luiz Carlos P. Albini , Michele N. Lima , "Identity-based key management in mobile ad hoc networks: techniques and applications", IEEE Wireless Communications, 2008.

[3] Anubha Goyal, Geetanjali Babbar, Chandigarh Group Of Colleges, Landran , "Lightweight Key Distribution for secure routing and secure information propagation – A Review", International Journal of Advanced Research in Computer Engineering & Technology, pp.862-865, 2015.

[4] Anil Kapil and Sanjeev Rana, "Identity-Based Key Management in MANETs using Public Key Cryptography", International Journal of Security,pp.1-8, 2009.

[5] Wei Liu, Wenjing Lou ,Yanchao Zhang, and Yuguang Fang, "Securing Mobile Ad Hoc Networks with Certificateless Public Keys", IEEE Transactions On Dependable And Secure Computing,pp. 1-15, 2006.

[6] Ditipriya sinha, Uma Bhattacharya, Rituparna Chaki, "RSRP: a robust secure routing protocol in manet", Foundations of computing and decision sciences,pp. 130-154, 2014.

[7] Arputharaj Kannan , Pandi Vijayakumar, Sudan Bose, "Chinese remainder Theorem based centralised group key management for secure multicast communication", IET Information Security, pp.1-9, 2012.

[8] Yang Xu, Wei Zhou and Guo-Jun Wang, "Multiway Tree-Based Group Key Management Using Chinese Remainder Theorem for Multi-Privileged Group Communications", Journal of Applied Science and Engineering, pp.81-92, 2014.

[9] Vinod Kumar, Pandey, Rajendra Kumar, "Centralized group key management scheme for secure multicast communication without re-keying", Cornell University Library, pp.1-7, 2016.

[10] Chin-Chen Chang , Lein Harn and Yanjun Liu , "An authenticated group key distribution mechanism using theory of numbers", International Journal Of Communication Systems, s2013.

[11] Janani, V. S., and M. S. K. Manikandan, "CRTKM: Chinese remainder theorem based key management scheme for securing ad-hoc networks", IEEE International Conference on Signal Processing Informatics Communication and Energy Systems (SPICES), 2015.

[12] Janani, V. S., and M. S. K. Manikandan, "Genetic-IDGKA: Genetic ID-Based Group Key Agreement Protocol for Large MANETs", Journal of Discrete Mathematical Sciences and Cryptography, 2015.