ISSN (Print) : 0974-6846
Indian Journal of Science and Technology, *Vol 9(39), DOI: 10.17485/ijst/2016/v9i39/92897, October 2016* ISSN (Online) : 0974-5645

Code based Secret Sharing Schemes for MANET

Padmavathi Guddeti[1], P. V. Siva Kumar[2*] and Appala Naidu Tentu[3]

[1]Department of H&S, VNR VJIET, Hyderabad, India; padmagvathi@gmail.com
[2]Department of Computer Science and Engineering, VNRVJIET, Hyderabad, India; sivakumarpasupuleti@gmail.com
[3]CR Rao AIMSCS, University of Hyderabad Campus , Hyderabad, India; naidunit@gmail.com

Abstract

Secret values sharing in MANET is computationally insecure and inconsistent because of its dynamic nature. Shamir`s proposal is well known prominent secret sharing schemes. But it does not provide a dynamic approach to the particular application. In the same distribution process nodes may join or leave the network and able to obtain the similar capabilities as initial nodes; further, the joined nodes gain the shares (updated shares) corresponding to the secret. Two additional features of proposed system are that it allows to implement threshold operations, one for distributing secret information with other nodes and the other is using our threshold schemes in key management. Secret values sharing in MANET is computationally insecure and inconsistent because of its dynamic nature. Proposed the group key establishment protocol operations in detail and also proposed two different methods for dealing network dynamic nature including adding and removing of the nodes..

Keywords: Interpolation, Key Generation, Key Management, MANETs, Threshold, Secret Sharing

1. Introduction

Mobile Ad-Hoc Networks[1] have ideal applications in different areas like military and civilian[2,3] such as surveillance in the battlefield. Different applications and areas of the WSN (wireless sensor networks) needs secure communications. However, Mobile Ad-Hoc Networks[4] are prone to dissimilar types of malicious attacks, such as masquerading, impersonating, interception for misleading because of the connectivity of wireless, the non availability of the physical protection and the unattended deployment. Thus, it is most important to implement security in sensor network is most important.

MANETs consist of dynamic nodes interconnected with wireless multi-hop communication paths[4]. In this network system, to communicate with each other the participating nodes do not need access points to reach another, by using a variety of routing protocols[5,6] the one participating node reaches another. Generally, in an ad hoc network routes among nodes may include multiple hops, thus it is suitable to call such networks as multi-hop wireless ad hoc networks. Within its transmission range, every node will be capable to interact directly with another node. The main security requirement[1,4] for MANETs is confidentiality, authentication, integrity, availability and non-repudiation.

Because mobile ad hoc networks have additional vulnerabilities than the traditional wired networks, thus security is not easy in the mobile ad hoc network.

Shamir[7] had suggested a scheme for splitting a sequence of data D into n different parts so that D can be rebuilt simply with k parts using Lagrange`s Interpolation method. This method enables the creation of strong key management designed for cryptographic system. A secret sharing scheme for an access structure is a technique in which a node is called dealer distributes secret shares to different participants such that (i) any subset shares can rebuild the secret, and (ii) any subset shares not in cannot acquire any information particularly about the secret in the theoretic sense of information. A secret sharing scheme[8] is ultimate if the secret selected from the same domain shareholders shares.

The key being secret brings many issues because of its constraint. Secret key storing with server or a person or database reduces the system security to the credibility and security of that manager. Moreover, not having a proper

* *Author for correspondence*

backup of the key leads the problem of losing the key if a misbehaviour takes place. On the other hand, if more than one manager holds the key, an enemy with a desire for the key has more flexibility of choosing the goal. To resolve these problems of key management, secret sharing schemes are introduced[8–10].

These schemes using an idea to share a secret with a set of managers such that only the coalitions of predefined can come together and disclose the secret, although no other coalition can get any information regarding the secret. Thus, the keys used in areas require extremely important secrecy like control mechanisms of nuclear systems, large-scale finance applications and command, can be stored by using secret sharing schemes[10]. Here, the secret is shared in the network to identify suspected nodes. By replacing private key for their equivalent public key encrypted[11] data, we can easily rebuild the original secret key.

2. Detection of Fake Shareholders (Cheaters)

A verifiable secret-sharing scheme[12] provides its shareholders with a capacity to validate that (i) every time the secret shares get from the dealer are copied from the same secret and (ii) the shares of secret get from the other share holder in the secret rebuild process are authentic shares. These characteristics are extremely important. For an example, some shareholders can fake by a corrupt dealer by assigning them fake shares. Noise or Communication errors can also consequence of fake shares. Also shareholder may cheat[25] others in the secret rebuilding procedure to prevent others from getting the original secret by presenting fake shares.

Sharing of the secret concept was first introduced by Blakley et al.[13,14] and Shamir[7]. Shamir[7] proposed scheme based on the standard Lagrange polynomial interpolation method, whereas the scheme by Blakley et al.[13,14] is based on the method of geometric that uses the concept of intersect hyper planes. Sarkar et al.[15] proposed Chinese Remainder Theorem, which is depends on RSA Threshold cryptography[16] in MANET using the scheme of Verifiable secret sharing. It develops Threshold cryptographic based schemes for mobile ad-hoc network. In the area of deterministic key pre-distribution, for a long time it uses the Chinese Remainder Theorem. Ravi et al.[17] anticipated attack resistant and capable key agreement scheme in MANET for secure group communication. For a group key generation this method also used CRT. The group key generation mechanism suffers from updating overhead because of the MANET dynamic nature.

Amuthan et al.[18] developed Sharing of secret for secure routing scheme in MANETs. This protocol implements a sharing of secret scheme using Shamir's secret sharing scheme[7] approach. Papadimitoras and Hass[19] designed Secure Data Transmission in MANET, which is depends on multiple paths. The main focus of the scheme is on robustness and privacy in communication. For privacy, to strengthen the data confidentiality a coding scheme using the XOR operation was recognized.

In our work we address the secret distribution to attain the distribution and privacy aspects of key management[20]. There exist a lot of scope for research in MANETs on security[21]. However, all security protocols are having some primary aspects that are very common. As the responsibility of a single node one can avoid those vital system events. Each node will be authenticated, authorized and non-repudiated. The Data sequence should be very confidential, so it cannot be changed easily[22]. Solutions provided by Threshold cryptography are essential help for aspect of security in MANET. In the literature, there are no computationally secured threshold cryptography considering such aspects. In this proposed scheme, we implement a method which would also be capable in point of the security aspects mentioned and it also would be more secured.

3. Verifiable Secret Sharing Scheme[23]

In this topic, we give details about verifiable secret sharing scheme which was addressed by Sivakumar et al.[23] is denoted as the initial set of n nodes in MANETs. In this protocol, centralized node is treated as a dealer. Which all other nodes connected to it act as participants. In this multi-secret sharing scheme, multiple of secrets having by the dealer which like to distribute with a certain number of nodes (participants) in the MANETs securely. In a sharing of secret scheme, a secret can be divided into shares, these schemes transmit information about the secret and need to be store securely. For secret reconstruction and verification, secret sharing also may use some public values associated with each player. Let set of n nodes involved in the sharing of secret. These

n participants denoted as p_1, p_2..., p_n and let a positive integer t such that $1 \le t \le n$. We fix a prime $q > n$, and n distinct points $a_1, a_2, ..., a_{t-1} \in F_q$. Let ($s_1$,$s_2$,....$s_k$) are the k pieces of secrets to be distributed to the participants of n.

In MANETs, server act as a dealer who runs initialization and distribution algorithms and let $s_1, s_2, ..., s_k$ represents k pieces of secrets to be distributed to participants of n. Previous to distribution phase, dealer uses the advantages of hash function and Identity based signature scheme. Each participant allocated with unique identity $ID_i, i = 1, 2, ..., n$. In this, a *Setup* polynomial time algorithm runs by a dealer that takes a security parameter 1^λ as inputs and outputs public parameters *params* and a master secret key *M S K* is as follows: $Setup(1^\lambda) \rightarrow (M\,S\,K,\ params)$.

Now the dealer runs polynomial time algorithm in which identity ID_i, public *params* and master secret key M S K takes as input and output a secret key $S K_{ID_i}$ associated to the identity ID_i is as follows:

$$KeyGen(ID_i, M\,S\,K,\ params) \rightarrow S\,K_{ID_i}.$$

Previous to the secret sharing, dealer sends secret key $S K_{ID_i}$ as secret shadows to the participants p_i securely. Then dealer randomly selects a value r and calculate $f(r, S K_{ID_i})$ for the values of $i = 1, 2, ..., n$.

The dealer shows how to execute the sharing of secret algorithm in two separate cases: when $k \le n$ and $k > n$. If pooling happens with atleast t or greater than t participants, then their secret shares will make it simple to rebuild the secrets, but secret share rebuild is not done by *t - 1* or lesser secret shares. In the information-theoretic sense, this scheme is an ideal threshold scheme in which significant only *t-1* or lesser secret shares gives no additional message about the secrets to an enemy.

Sivakumar et.al.[24] proposed three different secret sharing schemes for compartmental access structures.

3.1 Proposed Code-based Threshold Scheme

Given any set of k shares can determined the secret s where $s = (s_1, s_2, ..., s_k)$. And given any set of *k-1* and lesser shares gives nothing about the secret *s*. Let there are P_i participants where $1 \le i \le n$. Let S is secret space and T be the share space be the vector spaces over field F. Assume that $f : S \rightarrow T$ be the one to one share function to calculate shares for n participants. Let s=(s_1, s_2,..., s_k) be the vector space consisting of k secrets and T = (t_1, t_2, ...t_n) = f(s) the share given only to i^{th} participant is t_i.

3.1.1 Initialization Phase

- Choose a random prime number F as field.
- Choose maximum number of participants n and threshold value $k \in F$.
- Choose arbitrarily $s_i \in F$, $1 \le i \le k$ such that s_i is the i^{th} element in the secret space s.

3.1.2 Distribution Phase

- Let the vector $e_i \in F^k$ with the i^{th} entry being identity element 1 and other entries being the 0 element of F such that every $s \in F^k$ vector can be expressed as $s = \sum_{i=1}^{k} s_i e_i$.
- Compute the shares of participants by using the following share function:

$$f(s) = f\left(\sum_{i=1}^{k} s_i e_i\right) = \sum_{i=1}^{k} s_i f(e_i)$$
$$= sG = (t_1, t_2, ..., t_n),$$

where, G is $k \times n$ generator matrix, the rank of G is *k*. and $(t_1, t_2, ..., t_n) = T$ is the share vector.

- Distribute the shares to the n participants such that i^{th} participant gets the t_i^{th} share for $1 \le i \le n$.
- Publish the generator matrix.
- Choose any *k* (threshold value) columns of generator matrix to form a sub matrix $G(i_1, i_2, ..., i_u)$ where $i_1, i_2, ..., i_u$ are the $i_1^{th}, i_2^{th}, ..., i_u^{th}$ columns of given generator matrix and $1 \le u \le n$.
- Obtain the shares $t_{i_1}, t_{i_2}, ..., t_{i_u}$.
- Recover the secret vector s by solving the following linear equation:

$$sG(i_1, i_2, ..., i_u) = (t_{i_1}, t_{i_2}, ..., t_{i_u}).$$

4. Proposed Hierarchical Dynamic Threshold Scheme

4.1 Initialization

Dealer uses a Shamir scheme to distribute shares of an initial secret α_1 with threshold t_0 among players $P = \{p_1, p_2, ..., p_n\}$ and then he leaves the scheme. Suppose there are *m* levels {L_1, L_2,..., L_m} with set of players $\{n_1, n_2, ..., n_m\}$ and thresholds $\{t_1, t_2, ..., t_m\}$ corresponds to field F_q.

4.2 Sharing Phase

For each $i \in [1, m-1]$ repeat the following steps:

- The Players in the set P use polynomial production protocol, to generate a random secret β_i shares with threshold $t \in \min[t_i, t_{i+1}, ..., t_m]$
- Players n_i keeps shares of β_i shares as their final shares.
- Now $P = P - \{n_i\}$.

For level L_m:

Players in set P will calculate the following constant.

For $i \in [1, m-1]$, $\alpha_{i+1} = \alpha_i + \beta_i$.

After calculating $\{\alpha_2, \alpha_3, ..., \alpha_m\}$ they remain only shares of α_m as their final shares. Dynamically varying the Threshold at each level: Apply Lagrange Method for Threshold Modification Technique at each level from t_i to t_i', where $i \in [1, m-1]$

4.3 Recovery of the Secrets at Each Level

For $i \in [1, m-1]$. Now, if a set Δ_i' of at least t_i' participants cooperates, by using the method of Lagrange interpolation they can recover the secret: $Secret_i = \sum_{j \in \Delta_i'} \left(\gamma_j^{\Delta_i'} \times \varphi_j \right)$

Which was named as α_1. Now we got level wise secrets i.e. α_m from level m, β_{m-1} from level (m-1), β_{m-2} from level (m-2),……. β_1 from level 1.

Then by solving the following system of linear congruence:

$\alpha_{i+1} = \alpha_i + \beta_i \bmod q \quad for \quad i = (m-1)$

$down \quad from \quad level \quad i = 1.$

Therefore, $\alpha_1, ..., \alpha_1$ are recovered.

4.4 Polynomial Construction

- Initially, randomly select t players from P.
- Using Shamir scheme every t players P_i distributes a secret, called δ_i, $i \in [1, t]$ between the entire players, where *t*-1 is the degree of the polynomial secret sharing.
- Each player includes its shares of the δ_i s as one. As a outcome, every player has a their own share on t-1 degree polynomial *g(x)* with a constant term $\delta = \sum \delta_i$.

5. Threshold Change Algorithm by Lagrange Method

A set is fixed such that the set comprises of at least t designated players identifiers. Every player $P_i \in \Delta$ chooses random polynomial $g_i(x)$ of degree at most t-1 such that $g_i(0) = f(i)$. He then gives $g_i(j)$ to P_j for $1 \le j \le n$, i.e., re-sharing the original shares with supplementary shares.

The global constants are calculated as follows:

$$\gamma_j^{\Delta} = \prod_{j \in \Delta, j \neq i} \frac{j}{j-1} \quad for\ all\ i \in \Delta.$$

Every player $P_j (1 \le j \le n)$ replace its old shares, and then adds the supplementary shares which was received from other players to calculate its new share as given here: $\varphi_j = \sum_{i \in \Delta} \left(\gamma_j^{\Delta} \times g_i(j) \right)$.

6. Suggested Scheme Analysis

In the proposed scheme, generally, every share and participating node were verified by the verification scheme that participating nodes shares are consistent. Inconsistent shares cannot generate by the dealer in the sharing phase. If at least one of the verification equations does not satisfy then an inconsistent share generated by the dealer. In the reconstruction phase also verification scheme which is validated by the member of coalition S that all the participating nodes also cannot repudiate. If some node is repudiated, then there will be at least one not satisfied verification equation exists. In such a case, the false node is treated as malicious nodes. This is a cooperative approach where the i^{th} nodes share would be verified by the other alliance member. Hence, there is no scope of duplicitous by any malicious nodes. The participating nodes would get the secret value if all the shares are valid. The shared secret values always satisfy the validity, because in the coalition no adversary is able to participate easily. The node is identified as adversary when it is not satisfying the verification equation.

7. Discussion

We proposed a key management scheme in this paper

which make use of secret sharing schemes based on code based secret sharing schemes and dynamical secret sharing schemes based on polynomial interpolation proposed by Shamir's. The inner components of key management scheme are made by these secret sharing schemes. This key management is based on the SSS (Secret Sharing Scheme), in which the system secret is distributed to a group of server nodes. The server group creates a view of a CA (*Certification Authority)*. The advantage of key management is that it is easier for a node to request service from a well maintained group to a certain extent than from multiple independent service providers which may be spread in a large area. It is easier for servers to manage within the group rather than with the entire network throughout the secret share updating phase. Future, we integrate our proposed scheme to the key management approach.

8. References

1. Anjum F, Mouchtaris P. Security for wireless ad hoc networks. Wiley-Blackwell; Mar 2007.
2. Jesudoss A, Subramaniam NP. EAM: Architecting efficient authentication model for internet security using image-based one time password technique. Indian Journal of Science and Technology. 2016; 9(7). Doi no:10.17485/ijst/2016/v9i7/85017
3. Somassoundaram T, Subramaniam NP. High capacity image steganography using secret key for medical information. Indian Journal of Science and Technology. Jan 2016; 9(3). Doi no:10.17485/ijst/2016/v9i3/81455
4. Zhou L, Haas ZJ. Securing ad hoc networks. Cornell University: Securing ad hoc networks presented by Johanna Vartiainen. 1999; 1(26):24–30.
5. Revathi V, Pushpalatha M, Sornalakshmi K. Implementation of key exchange and secure routing mechanism in a wireless ad hoc testbeds. Indian Journal of Science and Technology. Mar 2016; 9(10). Doi no:10.17485/ijst/2016/v9i10/75998
6. K. Gomathi, B. Parvathavarthini. An Enhanced Distributed Weighted Clustering Routing Protocol for Key Management. Indian Journal of Science and Technology.2015 Feb; 8(4). Doi no:10.17485/ijst/2015/v8i4/60435
7. Shamir A. 1979. How to share a secret. Comm. ACM 22, 612–13.
8. Pranav Vyas, Bhushan Trivedi, Atul Patel. A Survey on Recently Proposed Key Exchange Protocols for Mobile Environment. Indian Journal of Science and Technology. 2015 Nov; 8(30). Doi no:10.17485/ijst/2015/v8i1/72068
9. Raju Barskar, Meenu Chawla. A Survey on Efficient Group Key Management Schemes in Wireless Networks . Indian Journal of Science and Technology. 2016 Apr; 9(14). Doi no:10.17485/ijst/2016/v9i14/87972
10. G. Jayamurugan, P. Kamalakkannan. Position-based Key Sharing with Higher Connectivity and Multivariate Optimized Resource Consumption in WSN. Indian Journal of Science and Technology. 2015 Dec; 8(35). Doi no: 10.17485/ijst/2015/v8i35/79969
11. Mehrnoush Toghian, Matei Ciobanu Morogan. Suggesting a Method to Improve Encryption Key Management in Wireless Sensor Networks. Indian Journal of Science and Technology. 2015 Aug; 8(18). Doino:10.17485/ijst/2015/v8i19/75986
12. Stadler M.(1996) Publicly verifiable secret sharing, Advances in Cryptology, EUROCRYPT-96, Lecture Notes in Computer Science. 1070. Springer-Verlag. 1996. p.190–99.
13. Blakley GR. (1979), Safeguarding cryptographic keys, AFIPS. 48. p.313–317.
14. Blakley GR, Kabatianski A. Ideal perfect threshold schemes and MDS codes, in IEEE Conf. Proc. Int. Symp. Information Theory. ISIT95, p.488. 1995.
15. Sarkar S, Kisku B, Misra S. and Obaidat MS.(2009) Chinese Remainder Theorem-Based RSA Threshold Cryptography in MANET using Verifiable Secret Sharing Scheme. IEEE International Conference on Wireless and Mobile Computing. Networking and Communications.
16. DI. George Amalarethinam, J. Sai Geetha, K. Mani. Analysis and Enhancement of Speed in Public Key Cryptography using Message Encoding Algorithm. Indian Journal of Science and Technology.2015 July; 8(16). Doi no: 10.17485/ijst/2015/v8i16/69809
17. Ravi K.Balachandan, Xukai Zou, Bytrav Ramamurthy, and AmardeepThukral, (2007) An efficient and attack resistant agreement scheme for secure group communications in mobile ad-hoc networks. Wireless Communication And Mobile Computing in Wiley Inter Science.
18. A.Amuthan and B.Arvind Baradwaj (2011) Secure Routing Scheme in MANETs using Secret Key Sharing. International Journal of Computer Applications(00975-8887). 22(1).
19. Papadimitoras and Hass.Z. (2003) Secure Data Transmission in Mobile Adhoc Networks, ACM workshop on Wireless Security, Proc.
20. R. Sarath, A. Shajin Nargunam. Key Distribution using Dual Channel Technique for Ultimate Security. Indian Journal of Science and Technology. 2015 Oct; 8(26). Doi no:10.17485/ijst/2015/v8i26/80999
21. Crescenzo GD, Ge R. and Arce GR. (2005) Improved Topology Assumptions for Threshold Cryptography in Mobile Ad Hoc Networks. 3rd ACM workshop on Security of ad hoc and sensor networks. p.53–62, Alexandria. VA, USA. November.
22. Hu YC, and Perrig A. (2004) A Survey of Security Wireless Ad Hoc Routing, IEEE Security and Privacy. 2(3); 28–39.
23. Siva Kumar PV. Rajasekhara Rao Kurra, and Appala Naidu Tentu ,Verifiable Secret Sharing protocol for Mobile Adhoc Networks. CiiT International Journal of Networking

and Communication Engineering. 6(2). February 2014. ISSN 0974 – 9616. p.35–40.

24. Siva Kumar PV. Rajasekhara Rao Kurra, Appala Naidu Tentu and Padmavathi .G. Multi-Level Secret Sharing Scheme for Mobile Ad-Hoc Networks. Published in Int. J. Advanced Networking and Applications 6(2); 2253–2261 (2014) ISSN : 0975-0290.
25. Pasaila D, Alexa V, and Iftene S. Cheating detection and cheater identification in crt-based secret sharing schemes. IACR Cryptology ePrint Archive. 2009. p 426.