Volume: 6 Issue: 2 Pages: 2253-2261 (2014) ISSN : 0975-0290

# Multi-Level Secret Sharing Scheme for Mobile Ad-Hoc Networks

**P.V. Siva Kumar**
Department of Computer Science and Engineering, VNR VJIET, Hyderabad, India
Email: sivakumarpasupuleti@gmail.com
**Dr. Rajasekhara Rao Kurra**
Sri Prakash College of Engineering, Tuni, India,
email: krr_it@yahoo.co.in
**Appala Naidu Tentu and G.Padmavathi**
CRRao AIMSCS, University of Hyderabad Campus, Hyderabad ,India
Email: naidunit@gmail.com, padmagvathi@gmail.com

**----------ABSTRACT----------**

In this paper, we are concerned with security for Mobile Ad-hoc Networks (MANETs) using threshold cryptography. When we are applying cryptography to MANETs, key management schemes must provide the cryptographic keys in a secure manner and storing the secret information within the nodes, thwarting the activities of malicious nodes inside a network and is how to distribute the role of the trusted authority among the nodes. Mobile ad hoc networks (MANETs) represent complex distributed systems that comprise wireless mobile nodes that can freely and dynamically self-organize into arbitrary and temporary, ad-hoc network topologies. Secret Sharing Scheme is a method which distributes shares of a secret to a set of participants in such a way that only authorized subset of participants can uniquely reconstruct the secret and an unauthorized subset can get no information about the secret. In this paper we present a new multilevel secret sharing scheme by extending the Shamir's to the case that the global threshold is strictly greater than the sum of the compartment thresholds and we indicate how to use the threshold secret sharing schemes based on polynomial interpolation. These schemes are based on one-way functions (Discrete Logarithm) which are computationally perfect. In the first scheme the number of public shares grows exponentially with the number of participants. To overcome this disadvantage we proposed two efficient schemes in which the number of public shares ate linearly proportional to the number of participants. Both these schemes are similar except that in the third scheme the identities of the participants are also hidden. In this we also addressed the problem of malicious shareholders that aim to corrupt a secret sharing scheme. To prevent such a threat, legitimate shareholders must detect any modification of shares that has not been issued by a node responsible for the sharing of secret S.

**Keywords - Compartmented access structure, computationally perfect, ideal, secret sharing scheme, Verifiable, MANETs.**

Date of Submission: July 29, 2014 Date of Acceptance: August 12, 2014

## 1. INTRODUCTION

A mobile ad hoc network (MANET) [3] is a set of mobile devices that are connected through wireless links. MANETs have characteristics such as limited bandwidth, absence of any fixed central structure, and ever changing topologies. Thus, implementing strong security services in such environments is very hard and MANETs are highly vulnerable to various security attacks [2]. To solve security problems, public key cryptography must be used in MANETs without incurring heavy network traffic. One of the main components of PKI infrastructure is a certificate authority (CA), it is a trusted third party used for issuing, revoking, and managing of user certificates. Unfortunately, the CA itself can be attacked and finally compromised; in this case, the intruder can sign certificates using the CAs private key.

Certificate authorities (CAs) are the main components of PKI that enable us for providing basic security services in wired networks and Internet. But, we cannot use centralized CAs, in mobile ad hoc networks (MANETs). So, many efforts have been made to adapt CA to the special characteristics of MANETs and new concepts such as distributed CAs (DCAs) have been proposed that distribute the functionality of CA between MANET nodes.

Key management system is an underlying mechanism for securing both networking functions (e.g., routing) and application services in mobile ad hoc networks. Public Key Infrastructure (PKI) has been recognized as one of the most effective tools for providing security for dynamic networks. However, providing such an infrastructure in MANETs is a challenging task due to their infrastructure less nature. Hence, the PKI in ad hoc networks are mobile hosts nodes (or a set of them), then the key management system should not trust nor rely on any fixed Certificate Authority CA, but should be self organized.

We identify two main challenges in distributing the CA functionality over multiple nodes. The first challenge

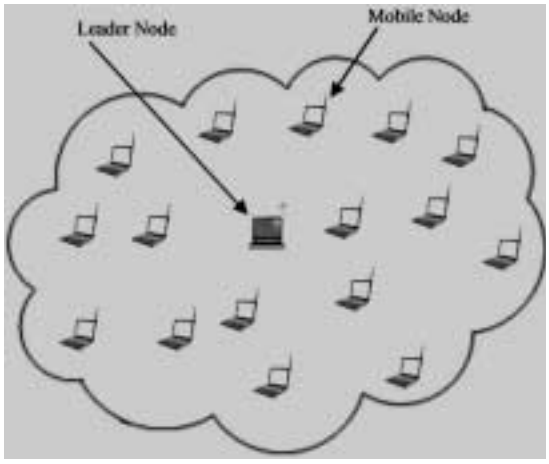
Volume: 6 Issue: 2 Pages: 2253-2261 (2014) ISSN : 0975-0290

[13] is picking a set of nodes to collectively provide the CA service. The second and equally important challenge is how to provide efficient and effective communication between the mobile nodes and the CA nodes, even in dynamic networks with possible compromises or temporary network partitions.

### 1.1 CHARACTERISTICS OF MANET

A MANET consists of mobile platforms (e.g., a router with multiple hosts and wireless communications devices)–herein simply referred to as"nodes"–which are free to move about arbitrarily. The nodes may be located in or on airplanes, ships, trucks, cars, perhaps even on people or very small devices, and there may be multiple hosts per router. A MANET is an autonomous system of mobile nodes. The system may operate in isolation, or may have gateways to and interface with a fixed network. In the latter operational mode, it is typically envisioned to operate as a "stub" network connecting to a fixed internetwork. Stub networks carry traffic originating at and/or destined for internal nodes, but do not permit exogenous traffic to "transit" through the stub network.

MANET nodes are equipped with wireless transmitters and receivers using antennas which may be unidirectional (broadcast), highly-directional (point-to-point), possibly steerable, or some combination thereof. At a given point in time, depending on the nodes' positions and their transmitter and receiver coverage patterns, transmission power levels and co-channel interference levels, a wireless connectivity in the form of a random, multi-hop graph or "ad hoc" network exists between the nodes. This ad hoc topology may change with time as the nodes move or adjust their transmission and reception parameters.




The concepts of threshold secret sharing [10], [4] and secret share updates are not new, and have been studied in the cryptography context. However, these proposals assume limited number of secret share holders, and are not scalable to network size. They typically involve excessive communication overhead, and assume a richly connected network topology.

Besides the scaling issue, these solutions do not work well in the mobile networking environment. They cannot satisfy the following two requirements for mobile networking security: (1) Mobile users demand anywhere, anytime ubiquitous security services, since they may freely roam. As long as the network condition is better than a predefined lower bound, security services should be available all the time. (2) Compared to wired networks, wireless networks are constrained by their unique features. Security services must be provided despite wireless channel error, network partitioning, and entity joins/leaves. For the above reasons, these existing solutions are not applicable to mobile networks with dynamic membership.

Secret sharing is a cryptographic primitive, which is used to distribute a secret among participants in such a way that an authorized subset of participants can uniquely reconstruct the secret and an unauthorized subset can get no information about the secret. It is a fundamental method used in secure multiparty computations, where various distrusted participants cooperate and conduct computation tasks based on the private data they provide. A secret sharing scheme is called ideal if the maximal length of the shares and the length of the secret are identical. Secret sharing was first proposed by Blakley [4] and Shamir[10]. The scheme by Shamir relies on the standard Lagrange polynomial interpolation, whereas the scheme by Blakley[4] is based on the geometric idea that uses the concept of intersecting hyper planes.

The family of authorized subsets is known as the access structure. An access structure is said to be monotone if a set is qualified then its superset must also be qualified. Several access structures are proposed in the literature. They include the *(t, n)* - threshold access structure, the Generalized access structure and the Multipartite access structure. In the *(t, n)* - threshold access structure there are *n* shareholders, an authorized group consists of any *t* or more participants and any group of at most *t - 1* participants is an unauthorized group.

Let U be a set of n participants and let $2^U$ be its power set. Then the 'Generalized access structure' refers to situations where the collection of permissible subsets of U may be any collection $\Gamma \in 2^U$ having the monotonicity property. In multipartite access structures, the set of players U is partitioned into m disjoint entities $U_1, U_2, \ldots, U_m$ called levels and all players in each level play exactly the same role inside the access structure.

Compartmented access structure is a multipartite access structure such that all subsets containing at least $t_i$ participants from $U_i$ for every $i$, $1 \leq i \leq m$, and a total of at least $t_0$ participants are qualified to reconstruct the sec Formally,

$\Gamma = \{V \subseteq U: |V \cap U_i| \geq t_i,$

$for\ every\ i \in \{1,2,..,m\} and\ |V| \geq t_0$, where $t_0 \geq \sum_{i=1}^{m} t_i,$

Volume: 6 Issue: 2 Pages: 2253-2261 (2014) ISSN : 0975-0290

This access structure was first proposed by Simmons[41]. It was later generalized it to this form by Brickell[23] and it is now known as the compartmented access structure with lower bounds [42], [43]. A secret sharing scheme is a perfect realization of $\Gamma$ if for all $A \in \Gamma$, the users in A can always reconstruct the secret and for all B not in $\Gamma$, the users in B collectively cannot learn anything about the secret, in the information theoretic sense.

### 1.2 THRESHOLD CRYPTOGRAPHY

In threshold cryptography, operations like the generation of digital signatures are divided among network nodes, so that the action can be done if at least a certain number of parties collaborate. It tolerates the crashes of some components, for example, a *(t-1, n)* threshold signature allows, in a group of a total of n parties, any *t* parties sign jointly, but no coalition of up to *t - 1* parties can. Any service provided by CA is performed jointly by $t(t \leq 2)$ CA nodes, where *t* is called the threshold of the secret sharing. In this way, even if an attacker has discovered the secret shares of some but less than *t* CA nodes, the attacker still cannot recover CAs secret key. However, the above threshold secret sharing scheme still fails when the shares of more than t, CA nodes have been discovered by the intruders over a sufficiently long period.

### 1.3 RELATED WORK

MANETs has several kinds of security issues, caused by their nature of collaborative and open systems and by limited availability of resources. On the other hand, the secret sharing method has been actively studied in the field of cryptography [10], [15], [44]. The advantage of using the secret sharing method is that the possibility of a single point of failure is significantly reduced. Moreover, the secret sharing method has been applied in mobile ad hoc networks, [15], proposed a distributed public-key management scheme based on threshold secret sharing in which the CA services are divided into a certain number of specialized servers. The drawback is that it assumes some nodes must behave as servers. When moving towards fully distributed infrastructure, a decentralized authentication protocol is developed to distribute the authentication of a certificate authority (CA) by utilizing secret sharing.

Simmons [41] introduced the compartmented access structure and presented ideal secret sharing schemes for some particular examples of this access structure [26]. These constructions are based on the generalization of the geometric method by Blakley [25]. Brickell also studied the compartmented access structure, generalized it to be called as compartmented access structure with lower bounds, and proposed a method based on vector space concepts to construct ideal secret sharing schemes [23]. A method that uses duality techniques to construct an ideal secret sharing scheme for compartmented access structure with lower bounds was suggested in [33].Constructions of ideal vector space secret sharing schemes for variants of the compartmented access structure and also for some tripartite access structure have been given in [21], [24], [27], [30], [33]. Almost all of these constructions require a huge number of determinants, which can grow exponentially on the number of participants, to be computed [25], [22], [33]. There are no known schemes for compartmented access structures that circumvent this problem [33].

Tassa [32] and Tassa and Dyn [33] proposed ideal secret sharing schemes, based on Birkhoff interpolation and bivariate polynomial interpolation respectively, for several families of multipartite access structures that contain the multilevel and compartmented ones. These schemes are perfect in a probabilistic manner [29].

Variants of the access structure called compartmented access structure with upper bounds and compartmented access structure with upper and lower bounds have also been introduced in [23], [26], [32]. Herranz and Saez [27] offered a family of ideal multipartite access structures that can be seen as a variant of the compartmented ones.

In 1994, He and Dawson [37] proposed a multistage secret sharing (MSS) to share multiple secrets based on one-way function. They used the public shift technique to obtain the true shadows and the successive applications of a one-way function to make the secrets reconstructed stage-by-stage in predetermined order. In their scheme, the secret holder publishes *pn* public values. In order to reduce the number of public values, Harn [35] proposed an alternative scheme which has a smaller number of public values than He and Dawsons scheme [37]. In Harns scheme [35], the secret holder publishes *p (n-t)* public values.

In 1995, He and Dawson [38] proposed a dynamic multi-secret sharing scheme based on two-variable one-way function. The two-variable one-way function is a good method to avoid disclosing the secret shadows. In a dynamic secret sharing scheme, the secret holder has the ability to publish some information about which secret he/she wants to share. All of the above schemes [35], [37], [38] use the one-way function and the polynomials of degree (t - 1) ([37], [38]) or (n-1) ([35]) to distribute secrets. Harn [36] proposed another threshold multi-secret sharing scheme which is based on the Lagrange interpolating polynomial and the DSA-type digital signatures [39], [40].

### 1.4 OUR CONTRIBUTION

In this paper, we focus on providing a secret sharing approach that is useful for compartmented (levels) infrastructure in MANETs. We inspire ourselves from the Ghodosi's [17] secret sharing schemes for compartmented groups. We present ideal secret sharing schemes for compartmented groups based on public information. Our proposed schemes are computationally perfect and based on one-way function (Discrete Logarithm). We also provide verification of the shares (cheating detection) provided by the participants in the reconstruction phase. We will further explore the multi-secret sharing aspect with the vision to apply our

Volume: 6 Issue: 2 Pages: 2253-2261 (2014) ISSN : 0975-0290

proposed method in a particular cluster- based architecture. In this kind of clustered topology, a node with more security privileges, called cluster head could be responsible for the generation, distribution and renewal of secret shares. The organization of the paper is as follows. In section 2 we will discuss some basic concepts related to MANETs and secret sharing. In Section 3 we describe a construction for computationally secure general secret sharing for compartmented groups based on public information. Section 4 describes compartmented secret sharing schemes used to avoid the disadvantage of the scheme described in section 3 and conclusions are in section 5.

## 2. BASIC CONCEPTS

Here we explain the definitions of some concepts used in this paper.

### 2.1 SECURITY REQUIREMENTS

The security services [2] of ad hoc networks are not altogether different than those of other network communication paradigms. The goal is to protect the information and the resources from attacks and misbehavior. In dealing with network security, we shall explain the following requirements that an effective security paradigm must ensure:

**2.1.1 Availability**: ensures that the desired network services are available whenever they are expected, in spite of attacks. Systems that ensure availability seek to combat denial of service and energy starvation attacks that we will present later.

**2.1.2 Authenticity:** ensures communication from one node to another is genuine. It ensures that a malicious node cannot masquerade as a trusted network node.

**2.1.3 Data confidentiality**: is a core security primitive for ad hoc networks, It ensures that a given message cannot be understood by anyone else than its (their) desired recipient(s). Data confidentiality is typically enabled by applying cryptography.

**2.1.4 Integrity**: denotes the authenticity of data sent from one node to another. That is, it ensures that a message sent from node A to node B was not modified by a malicious node, C, during transmission. If a robust confidentiality mechanism is employed, ensuring data integrity may be as simple as adding one-way hashes to encrypted messages.

**2.1.5 Non-repudiation:** ensures that the origin of the message is legitimate. i.e when one node receives a false message from another, nonrepudiation allows the former to accuse the later of sending the false message and enables all other nodes to know about it. Digital signature may be used to ensure nonrepudiation

### 2.2 SECURITY CONSIDERATIONS [1]

Without some form of network-level or link-layer security, a MANET routing protocol is vulnerable to many forms of attack. It may be relatively simple to snoop network traffic, replay transmissions, manipulate packet headers, and redirect routing messages, within a wireless network without appropriate security provisions. While these concerns exist within wired infrastructures and routing protocols as well, maintaining the ”physical” security of of the transmission media is harder in practice with MANETs. Sufficient security protection to prohibit disruption of modification of protocol operation is desired. This may be somewhat orthogonal to any particular routing protocol approach, e.g. through the application of IP Security techniques Mobile wireless networks are generally more prone to physical security threats than are fixed, hardwired networks. Existing link-level security techniques (e.g. encryption) are often applied within wireless networks to reduce these threats. Absent link-level encryption, at the network layer, the most pressing issue is one of inter-router authentication prior to the exchange of network control information. Several levels of authentication ranging from no security (always an option) and simple shared-key approaches, to full public key infrastructure based authentication mechanisms will be explored by the group. As an adjunct to the working groups efforts, several optional authentication modes may be standardized for use in MANETs.

### 2.3 SHAMIR’S (t, n) THRESHOLD SECRET SHARING SCHEME

In this sub section, we review Shamir`s [10] threshold secret sharing scheme. Then, we give some fundamental definitions of hierarchical threshold secret sharing scheme and compartmented threshold secret sharing schemes.

The Shamir [10] (t, n) threshold scheme uses polynomial interpolation. Let secrets be taken from the set $S \in GF_q$ where $GF_q$a finite Galois field with q elements is. Shamir scheme uses two algorithms: the dealer and combiner. The dealer sets up the scheme and distributes shares to all participants $P = \{P_1, P, \dots, P_n\}$ via secure channels. The combiner collects shares from collaborating participants and computes the secret only if the set of cooperating participants is of size t or more. To set up a (t, n) threshold scheme the dealer chooses n distinct nonzero elements $x_1, x_2, \dots x_n \in GF_q$ and publishes them. Next for a secret S, the dealer randomly chooses *t-1* elements $a_1, a_2, \dots, a_{t-1}$ from $GF_q$ and forms the following polynomial

$$f(x) = S + \sum_{i=1}^{t-1} a_i x^i.$$

The share of participant $P_i$ is $S_i = f(x_i)$. The secret $S = f(0)$. Note that $a_i$ are randomly chosen from all elements of $GF_q$, so in general, f(x) is of degree at most t - 1. During the reconstruction phase, the combiner takes

Volume: 6 Issue: 2 Pages: 2253-2261 (2014) ISSN : 0975-0290

shares of at least *t* participants $S_{i_1}, S_{i_2}, \ldots, S_{i_t}$ , and solves the system of equations to recovery the secret.

The Lagrange interpolation formula gives the expression for the secret S. It is known that the Shamir scheme is perfect. That is, if a group of fewer than t participants collaborate, their original uncertainty about S remains unchanged.

### 2.4 GHODASI [17] COMPARTMENTED SECRET SHARING SCHEME

Let the set of participants P be partitioned into $l$ disjoint$P_1, P, \ldots, P_l$ sets. The proposed secret sharing scheme for compartmented access structure as follows. The numbers of participants in different compartments and integers $t, t_1, t, \ldots, t_l$ determine an instance of the compartmented access structure.

We consider two distinct cases:

**Case (1)**: $t = \sum_{i=1}^{l} t_i$

In this case the compartmented access structure is:

$$\Gamma = \{A \subseteq P: |A \cap P_i| \geq t_i, for \;\; i \in \{1,2,..,l\}$$

A trivial solution for the above access structure is as follows. The dealer simply chooses $l$ - *1* random values $c_1, c_2, \ldots, c_{l-1}$from elements of GF(q), and defines a polynomial,

$$k(x) = K + c_1 x + c_2 x^2 + \cdots + c_{l-1} x^{l-1}$$

The secret $K = k(0)$and the partial secrets $k_i = k(i)$ for $i \in \{1,2,..,l\}$. In this scheme dealer constructs a Shamir$(t_i, n_i)$ scheme for each compartment *i*. The schemes are independently designed and the scheme in the *i-th* compartment allows to recover the partial key $k_i$. The collections of shares for all compartments are later distributed securely to the participants. Obviously, if at least ti participants of the *i-th* compartment pool their shares, they can reconstruct the partial secret $k_i$. A group of fewer than $t_i$collaborating participants learns absolutely nothing about $k_i$. Thus, the reconstruction of the secret K needs all partial keys to be reconstructed by at least $t_i$ participants in each compartments *i*.

**Case(2):** $t > \sum_{i=1}^{l} t_i$ In this case, the corresponding access structure is:

$$\Gamma = \{A \subseteq P: |A| \geq t, |A \cap P_i| \geq t_i, for \;\; i \in \{1,2,..,l\}$$

Let $T = t - \sum_{i=1}^{l} t_i$ The secret sharing scheme for above mentioned compartmented access structure is given in [17].

## 3. GENERAL SECRET SHARING FOR COMPARTMENTED GROUPS

We develop the secret sharing method in a fully distributed manner: Each collector node acts as the dealer node as defined in the secret sharing scheme [10] and is responsible to distribute the decryption key of its own data. Based on the architecture of MANETs, every node in the MANET is having the unique address. In a network, any node is ac ting as a source and destination remaining all other nodes in the region is to be considered as routers. Thus, in order to identify the secret shares that belong to the same key, the collector node will generate a unique key ID to append to each key share. The unique key ID will help to identify the secret shares that belong to the authorized set or not in the reconstruction phase.

In this section we describe a construction for computationally secure general secret sharing scheme for compartmented groups based on public information. Let S be the secret and n be the total number of participants and $l$ be the number of levels. Let $n_1, n_2, \ldots, n_l$ be the number of participants in each level. Let $t_1, t_2, \ldots, t_l$be the threshold for each level and t be the global threshold. The secret sharing method splits the keys into multiple shares and distributes them to multiple nodes, which brings the challenge that due to node mobility, these key shares may not be available in the neighborhood when they are needed for secret re-construction.

### 3.1 Distribution Phase

**3.1.1** Choose *l-1* random values

$c_1, c_2, \ldots, c_{l-1} \in GF_q$

and define a polynomial of $s(x) = s + c_1 x + c_2 x^2 + \cdots + c_{l-1} x^{l-1}$.The secret S = S(0) and the partial secrets $s_i = s(i)$ for $i = 1,2, \ldots, l$. For each compartment generate the authorized subsets.

**3.1.2** For all participants in each compartment randomly generate the secret shares$se_1, se_2, \ldots, se_{n_i} \in GF_q, 1 \leq i \leq l$ and secretly send them to all participants.

**3.1.3** Choose an arbitrary one-way function f(x).For each authorized subset A in every compartment compute and broadcast the public shares

$T_A = s_i - f(\sum_{i \in A} se_i),\ 1 \leq i \leq l$

### 3.2 Recovery Phase

**3.2.1** All the t participants will submit their secret shares $se_j$ along their group public shares$T_A$.

**3.2.2** From this information the partial secret for each compartment is calculated as $s_i = f(\sum_{i \in A} se_i) + T_A)$.

**3.2.3** Knowing the partial secrets, the secret S can be recovered.

This technique is useful to provide a shared secret to legitimate nodes in a infrastructure-less mobile ad-hoc network (MANET).

This scheme is having the disadvantage that a large amount of information must be broadcasted and authenticated. The complexity of this scheme is increased exponentially as the number of participants are increased

Volume: 6 Issue: 2 Pages: 2253-2261 (2014) ISSN : 0975-0290

i.e., the number of public shares are exponentially increased with the number of participants. To overcome this disadvantage we propose the following two schemes in which the numbers of public shares are linearly proportional to the number of participants.

**Theorem 3.1:** The proposed secret sharing scheme is ideal and is computationally perfect.

**Proof:** In this scheme each participant is given exactly one secret share although each participant is having more than one public share. As we can see all of shares are from the same domain as the secret the proposed secret sharing scheme is ideal. This scheme allows to reconstruct the secret only if the collaborating participants form an authorized subset for each compartment. Note that to reconstruct the secret S each compartment needs to reconstruct its associated partial secret $S_i$. At least $t_i$ participants from each compartment must participate in order to reconstruct the secret. Let this authorized subset be *A*. All the participants in *A* must submit their secret shares along with their group public share. By using the secret shares the combiner first calculate $m = (\sum_i se_i)$ where $se_i \in A$. Then one way hash function which is used in the distribution phase is applied to m. The result is then added to the group public share to obtain the partial secret$S_i$. By using these partial shares we can reconstruct the original secret S. An unauthorized subset B cannot compute m. So the members of B cannot compute $S_i$ by themselves.

## 4. EFFICIENT SECRET SHARING SCHEMES FOR COMPARTMENTED GROUPS

Compartmented access structure is a multipartite access structure such that all subsets containing at least $t_i$ participants from $U_i$ for every i (i is varies between 1 to m, m is number of compartments) and a total threshold of at least $t_0$ participants are qualified to reconstruct the secret.

### 4.1 SECRET SHARING SCHEME WITHOUT HIDING THE IDENTITIES OF THE PARTICIPANTS

Let S be the secret, n be the total number of participants and $l$ be the number of levels. Let $n_1, n_2, \dots, n_l$ be the number of participants in each level. Let $t_1, t_2, \dots, t_l$ be the threshold for each level and t be the global threshold. It is worth emphasizing here that the shares have to be distributed securely (encrypted) in order to guarantee data integrity, and that t still needs to be authenticated. In other words, the shares have to be created and shared by only legitimate MANET nodes in order to avoid malicious nodes to reconstruct S using the broadcasted public information. To enable such functionalities, we could for instance use a pre-shared key which is only used for the initial distribution of the shares.

#### 4.1.1 DISTRIBUTION PHASE

To share the secrets $se_1, se_2, \dots, se_n$among the n participants $p_1, p_2, \dots, p_n$ In distribution phase the dealer performs the following steps:

**1)** Randomly choose n integers $se_1, se_2, \dots, se_n$and also choose another $l$ secrets so that $s_1 + \cdots + s_n = S$

**2)** For each level $i, 1 \le i \le l$choose $t_i - 1$ random values and generate the polynomial

$f_i(x_j) = s_i + a_{i_1}x + \cdots + a_{i_{t_i-1}}x^{t_i-1} \quad 1 \le i \le l, 1 \le j \le t_i$

and compute $f_i(x_j)$ values for all *n* users.

**3)** Compute $h_{ij} = g^{se_j} \bmod q$ for all *n* users $1 \le i \le l, 1 \le j \le t_i \quad g \in GF_q$and $g$ made as public.

**4)** Then compute $d_{ij} = f_i(x_j) - h_{ij}$

**5)** Send the individual secret values $se_1, se_2, \dots, se_n$ to *n* participants securely and publish $d_{ij}$.

#### 4.1.2 RECOVERY PHASE

There must be at least $t_i$collaborating participants from each compartment. Let the actual numbers *P* of collaborating participants be $\alpha_1, \alpha_2, \dots, \alpha_l$ such that $\alpha_l \ge t_i$ and $\sum_{i=1}^{l} \alpha_i > t$

**1)** At least $t_i$ participants from each compartment must submit their $h_{ij}$ values.

**2)** The combiner calculates $f_i(x_j)$ for each participant using $h_{ij}$ and public values $d_{ij} = f_i(x_j)$

**3)** Then the combiner can establish the following system of linear equations:

$$s_1 + a_{11}x_{l_1} + a_{12}x_{l_1}^2 + \cdots + a_{1t_1-1}x_{l_1}^{t_1-1} = f_1(1)$$
$$s_1 + a_{11}x_{l_2} + a_{12}x_{l_2}^2 + \cdots + a_{1t_1-1}x_{l_2}^{t_1-1} = f_1(2)$$
$$\cdots\cdots\cdots\cdots$$
$$s_1 + a_{1\alpha_1}x_{l_1} + a_{12}x_{l_{\alpha_1}}^2 + \cdots + a_{1t_1-1}x_{l_{\alpha_1}}^{t_1-1} = f_1(\alpha_1)$$
$$\cdots\cdots\cdots\cdots\cdots$$
$$s_l + a_{l1}x_{l_1} + a_{l2}x_{l_1}^2 + \cdots + a_{lt_1-1}x_{l_1}^{t_1-1} = f_l(1)$$
$$s_l + a_{l1}x_{l_2} + a_{l2}x_{l_2}^2 + \cdots + a_{lt_1-1}x_{l_2}^{t_1-1} = f_l(2)$$
$$\cdots\cdots\cdots\cdots$$
$$s_l + a_{l\alpha_1}x_{l_1} + a_{l2}x_{l_{\alpha_1}}^2 + \cdots + a_{lt_1-1}x_{l_{\alpha_1}}^{t_1-1} = f_l(\alpha_l)$$

**4)** The combiner will solve the above equations and get the values of the partial secrets $s_1, s_2, \dots, s_l$ . From these we can recover the original secret *S* by adding all the partial secrets $s_1, s_2, \dots, s_l$

Volume: 6 Issue: 2 Pages: 2253-2261 (2014) ISSN : 0975-0290

### 4.2 SECRET SHARING SCHEME BY HIDING THE IDENTITIES OF THE PARTICIPANTS

This scheme is same as above but here identities of the participants are hidden.

#### 4.2.1 DISTRIBUTION PHASE

**1)** Let l be the number of levels and n be the number of participants. Randomly choose n integers $se_1, se_2, \dots, se_n$ and also choose another $l$ secrets so that $s_1 + \cdots + s_n = S$

**2)** For each level $i, 1 \le i \le l$, choose $t_i - 1$ random values and generate the polynomial

$$f_i(x_j) = s_i + a_{i_1}x + \cdots + a_{i_{t_i-1}}x^{t_i-1},$$
$$1 \le i \le l, 1 \le j \le t_i$$

and compute $f_i(x_j)$ values for all $n$ users.

**3)** Compute $h_{ij} = g^{se_j} \bmod q$ for all $n$ users $1 \le i \le l, 1 \le j \le t_i$ $g \in GF_q$ and $g$ made as public

**4)** Then compute

$$d_k = f_i(h_{ij}), 1 \le i \le l, 1 \le j \le t_i, 1 \le k \le n$$

**5)** Send the individual secret values $se_1, se_2, \dots, se_n$ to $n$ participants securely and publish $y_1, y_2, \dots, y_n$ for all users in every compartment. The points are $(h_{ij}, y_k)$, $1 \le i \le l, 1 \le j \le t_i, 1 \le k \le n$.

#### 4.2.2 SECRET RECOVERY:

**1)** At least $t_i$ participants from each compartment submit their $h_{ij}$ values.

**2)** By using the Lagrange interpolation polynomial the combiner generates the $t_i - 1$ degree polynomial

$$1 \le i \le l, \sum_{i=1}^{t_i} y_i \prod_{j=1, j\neq i}^{t_i} \frac{x - h_{ij}}{h_{ii} - h_{ij}}$$

After solving the above equation we get the following equation:

$s_i + a_{i_1}x + \cdots + a_{i_{t_i-1}}x^{t_i-1}$. From this we can Obtain the partial secret for every compartment.

**3)** Finally, we get the secret $s_1 + \cdots + s_n = S$

#### 4.2.3 SECURITY ANALYSIS

Following theorem establish that the proposed scheme is ideal and always recovers the secret in polynomial time if and only if the set of participants is an authorized set.

**Theorem 4.1:** The secret can be recovered by the recovery phase described above in polynomial time if and only if the set of participants recovering the secret is an authorized set.

**Proof:** In this scheme each participant is given exactly one secret share although each participant is having more than one public share. As we can see all of shares are from the same domain as the secret the proposed secret sharing scheme is ideal. This scheme allows reconstructing the secret only if the collaborating participants form an authorized subset for each compartment. Note that to reconstruct the secret S each compartment needs to reconstruct its associated partial secret $S_i$. At least $t_i$ participants from each compartment must participate in order to reconstruct the secret. Let this authorized subset be A. All the participants in A must submit their secret shares along with their group public share. By using the secret shares the combiner first calculate $m = (\sum_i se_i)$ where $se_i \in A$. Then one way hash function which is used in the distribution phase is applied to m. The result is then added to the group public share to obtain the partial secret $S_i$.

By using these partial shares we can reconstruct the original secret S. An unauthorized subset B cannot compute m. So the members of B cannot compute $S_i$ by themselves.

Above argument can also be extended for the other type of unauthorized set. Therefore, the secret can be recovered in polynomial time if and only if the set of participants recovering the secret is an authorized set.

## 5. CONCLUSION

In this work, we proposed a framework to facilitate secure data access in mobile wireless networks, where cryptographic keys. Three secret sharing schemes are proposed for Compartmented access structures. All these schemes are ideal and are computationally perfect and is based on the one-way function. By computationally perfect, we mean, an authorized set can always reconstruct the secret in polynomial time whereas for an unauthorized set this is computationally hard. This is in contrast to the majority of the schemes found in the literature, which are perfect in the probabilistic manner. A scheme is perfect in the probabilistic manner if either an authorized set may not be able to reconstruct the secret or an unauthorized set may be able to reconstruct the secret with some probability. In the first scheme the number of public shares grows exponentially with the number of participants. To overcome this disadvantage we proposed two efficient schemes in which the number of public shares ate linearly proportional to the number of participants. Both these schemes are similar except that in the third scheme the identities of the participants are also hidden. In this we also addressed the problem of malicious shareholders that aim to corrupt a secret sharing scheme. To prevent such a threat, legitimate shareholders must detect any modification of shares that has not been issued by a node responsible for the sharing of secret S.

## ACKNOWLEDGEMENTS

The authors acknowledge the financial support of this work from the DST WOS-A of India (Grant Sanction No.100/ (IFD)/2139/2012-13 dated 10.07.2012). Partially supported by CMS-DSTGOI project Lr.No SR/S4/MS: 516/07 dated 21.04.2008.

Volume: 6 Issue: 2 Pages: 2253-2261 (2014) ISSN : 0975-0290

**REFERENCES**


[1].Jiejun Kong and Petros, Z. and Haiyun Luo and Songwu Lu and Lixia Zhang., Providing Robust and Ubiquitous Security Support for Mobile Ad Hoc Networks. *In Proceedings of the Ninth International Conference on Network Protocols (ICNP '01)*. IEEE Computer Society, Washington, DC, USA, 251-260,2001.

[2]. William Stallings. Cryptography and Network Security principles and practices. *Pearson Education Inc*, third edition edition, 2003.

[3]. F. Anjum and P. Mouchtaris, Security for wireless ad hoc networks. *Wiley-Blackwell*, Mar. 2007.

[4]. Blakley, G. R., Safeguarding cryptographic keys. *In: AFIPS conference proceedings*, vol. 48, 313 - 317, 1979.

[5].R.-J. Hwang, C.-C. Chang, An on-line secret sharing scheme for multi secrets, *Computer Communications* 21 (13) (1998) 11701176.

[6].M.H. Dehkordi, S. Mashhadi An efficient threshold verifiable multi-secret sharing, *Computer Standards and Interfaces*, 30 (2008), pp. 187190.

[7].G Polymerou, EA Panaousis, E Pfluegel, C Politis, A novel lightweight multi-secret sharing technique for mobile ad-hoc networks, *29th Wireless World Research Forum (WWRF)*, Berlin, Germany, 2012.

[8].C.W. Chan and C.C. Chang, A Scheme for Threshold Multi secret Sharing, *Applied Mathematics and Computation*, Vol. 166, No.1, pp.1-14, 2005

[9]. Chien, H. Y., Jan, J. K., and Tseng, Y. M., "A practical (t,n) multi-secret sharing scheme", *IEICE Trans. Fundamentals* E83-A (12), 2000,pp. 2762-2765.

[10]. Shamir, A. 1979. How to share a secret. Comm. *ACM* 22, 612-613.

[11]. C.-C. Yang, T.-Y. Chang, M.-S. Hwang, A (t,n) multi-secret sharing scheme, *Applied Mathematics and Computation*, 151 (2004) 483490.

[12]. V. Daza, J. Herranz, P. Morillo, and C. Rafols, Cryptographic techniques for mobile ad-hoc networks, Computer Networks, *Elsevier*,vol. 51, no.18 , pp. 4938-4950, 2007.

[13]. H. Yang, H. Luo, F. Ye, S. Lu, and L. Zhang, Security in mobile ad hoc networks: challenges and solutions, *IEEE Wireless Communications*, vol. 11, no. 1, pp. 3847, Feb. 2004.

[14]. J. Zhao, J. Zhang, R. Zhao, A practical verifiable multi-secret sharing scheme, *Computer Standards and Interfaces* 29 (1) (2007) 138141.

[15]. L. Zhou and Z. Haas, Securing ad hoc networks, *IEEE Network*, vol. 13, no. 6, pp. 2430, Nov./Dec. 1999.

[16]. Chien, H.-Y., Jan, J.-K., Tseng, Y.-M.: A practical (t,n) multi-secret sharing. IEICE Transactions on Fundamentals of Electronics, *Communications and Computer Sciences* E83-A(12), 27622765 (2000).

[17]. Ghodosi, H., Pieprzyk, J., Safavi-Naini, R., Secret sharing in multilevel and compartmented groups. in: *Proc. ACISP 1998, LNCS*, vol. 1438,367 - 378, *Springer Verlag*, 1998

[18]. C. Cachin. On-line secret sharing. In C. Boyd, editor, Cryptography and Coding, *5th IMA Conference*, volume 1025 of *Lecture Notes in Computer Science*, pages 190198. Springer-Verlag, 1995.

[19]. Mitra Fatemi, Taraneh Eghlidos, Mohammadreza Aref, An Efficient Multistage Secret Sharing Scheme Using Linear One-way Functions and Bilinear Maps

[20]. Chou-Chen Yang, Ting-Yi Chang, Min-Shiang Hwang, A (t, n) multisecret sharing scheme in *Applied Mathematics and Computation* 151 (2004) 483490.

[21]. Beimel, A., Tassa, T.,Weinreb, E., Characterizing ideal weighted threshold secret sharing, *SIAM J. Disc. Math.*, 22 (1), 360 - 397, 2008.

[22]. Blakley, G. R., Kabatianski, A., Ideal perfect threshold schemes and MDS codes, in *IEEE Conf. Proc., Int. Symp. Information Theory*, ISIT95,p. 488, 1995.

[23]. Brickell, E. F., Some ideal secret sharing schemes, *J. Comb. Math.Comb.Comput.*, 9, 105 - 113, 1989.

[24]. Collins, M. J., A note on ideal tripartite access structures, manuscript available at http://eprint.iacr.org/2002/193/2002.

[25]. Farras,O., Marte-Farre, J.,Padro,C., Ideal multipartite secret sharing schemes, In:Naor,M.(ed.) *EUROCRYPT* 2007, LNCS, Vol.4515, pp.448-465, *Springer*, Heidelberg(2007).

[26]. Farras, O., Padro, C., Xing, C., Yang, A., Natural generalizations of threshold secret sharing, In:Lee, D. H., and Wang, X.(eds) *Asiacrypt* 2011. *LNCS*, Vol. 7073, pp. 610 - 627, 2011.

[27]. Herranz,J., Saez,G., New results on multipartite access structures, *IEEE Proc.Inf.Secur*.153, 153-162, 2006.

[28]. Karnin, E. D., Greene, J. W., Hellman, M. E., On secret sharing systems,*IEEE Trans. Inf. Theory*, IT-29, pp. 35 - 41, 1983.

[29]. Kaskaloglu, K., Ozbudak, F., On hierarchical threshold access structures, IST panel symposium, Tallinn, Estonia, Nov. 2010, (www.rto.nato.int/Pubs/rdp.asp?RDP=RTO-MP-IST-091).

[30]. Ng,S.-L, Ideal Secret Sharing Schemes with multipartite access structures, *IEEE Proc.commun.*153,165-168, 2006.

[31]. Josef Pieprzyk, and Xian-Mo Zhang, Ideal threshold schemes from MDS codes, *Proc. 5th Intl. Conf. Inf. Security and Cryptography*, LNCS,vol.2587, pp. 253 - 263, 2003.

[32]. Tamir Tassa., Hierarchical Threshold Secret Sharing, *Journal of Cryptology*, 20, pp. 237-264, 2007.

[33]. Tamir Tassa and Nira Dyn., Multipartite Secret Sharing by Bivariate Interpolation. *Journal of Cryptology*, 22, pp. 227-258, 2009.

Volume: 6 Issue: 2 Pages: 2253-2261 (2014) ISSN : 0975-0290

[34]. Yuyin Yu and Mingsheng wang., A Probabilistic secret sharing scheme for a compartmented access structure, In proceedings of the *13th international conference on Information and communications security*, (ods.)SihanQing, Willysusilo, Guilin wang,Dongmei liu, Springer- Verleg,PP.136-142,2011.

[35]. L. Harn, Comment: Multistage secret sharing based on one-way function,Electronics Letters 31 (4) (1995) 262.

[36]. L. Harn, Efficient sharing (broadcasting) of multiple secret, *IEEE ProceedingsComputers and Digital Techniques* 142 (3) (1995) 237240.

[37]. J. He, E. Dawson, Multistage secret sharing based on one-way function, *Electronics Letters* 30 (19) (1994) 15911592.

[38]. 1. J. He, E. Dawson, Multi-secret sharing scheme based on one-way function, *Electronics Letters* 31 (2) (1995) 9395.

[39]. M.-S. Hwang, C.-C. Chang, K.-F. Hwang, An ElGamal-like cryptosystem for enciphering large messages, *IEEE Transactions on Knowledge and Data Engineering* 14 (2002) 445446.

[40]. M.-S. Hwang, C.-C. Lee, Eric J.-L. Lu, Cryptanalysis of the batch verifying multiple DSA-type digital signatures, Pakistan *Journal of Applied Sciences* 1 (3) (2001) 287288.

[41]. G.J.Simmons., How to (Really) Share a secret, *Advances in Cryptology-CRYPTO'88, LNCS*, 403 (1990), 390-448.

[42]. Tamir Tassa and Nira Dyn., Multipartite Secret Sharing by Bivariate Interpolation. *Journal of Cryptology*, 22, pp. 227-258, 2009.

[43]. Farras, O., Padro, C., Xing, C., Yang, A., Natural generalizations of threshold secret sharing, *Asiacrypt 2011. LNCS*, Vol. 7073, pp. 610 - 627, 2011.

[44]. Asda . H. Stanis, A. Herzberg, H. Krawczyk, and M. Yung. 'Proactive secret sharing or: How to cope with perpetual leakage'. Pages 339–352. Springer-Verlag, 1995

**Authors Biography**

**P.V.Siva Kumar** received the Master of Computer Applications from JNTU Hyderabad in 1999 and M.Tech Degree in Computer Science and Engineering from Vinayaka Missions University in 2007. Now pursuing PhD in Computer Science and Engineering from Acharya Nagarjuna University, Guntur, Andhra Pradesh, India. He is presently working as Associate Professor in CSE Department at VNR VJIET Hyderabad. His current research interests Computer Networks, Network Security and Information Security. He is a life member of CSI and ISTE.

**Dr. Raja Sekhara Rao Kurra**. He is working as Director, Sri Prakash College of Engineering, Tuni, Andhra Pradesh, India. He did his MS in BITS Pilani and Ph.D in Acharya Nagarjuna University. He has 27 years of teaching experience. He published more than 30 technical papers in International Journals and more than 25 technical papers in National Journals and International Conferences. He received "Best Teacher Award" five times in the years 1998-1999, 2003-2004, 2004-2005, 2005-2006 and 2006-2007. Rajasekhara Rao Kurra received the Best Dean of the Year 2012 Award from The Association of Scientists, Developers and Faculty (ASDF), Government of Puducherry. He is the life member of ISTE and CSI and fellow of the IETE.

**T A Naidu** received the M.Tech in CSE from National Institute of Technology, Karnataka (NITK), Suratkal in 2010 and obtained M.Sc in Applied Mathematics from Andhra University Campus n 2007. He is pursuing PhD in Computer Science and Engineering from JNTU Hyderabad, Andhra Pradesh, India. He is presently working as Research Scientist in CR Rao AIMSCS, University of Hyderabad Campus. His current research interests are Design and Analysis of Cryptographic Protocols, Network Security and Information Security. He is a life member of CRSI and IACR.

**G. Padmavathi** received Gold medal in M.Sc (Maths) from Acharya Nagarjuna University, Guntur,Andhra pradesh in 2000 and received M.Phil from Madurai kamaraj University, Tamil Nadu in 2003 and submitted Ph.D dissertation at JNTUH University, Hyderabad in 2013.Currently working in DST WOS-A project as Women Scientist at CRRao AIMSCS, Hyderabad, India. Research interest includes Differential Equations, Modeling and Analysis, Neural networks, Cryptology.