Available online at www.sciencedirect.com
ScienceDirect
Electronic Notes in Theoretical Computer Science
ELSEVIER
Electronic Notes in Theoretical Computer Science 171 (2007) 33–41
www.elsevier.com/locate/entcs

On Dynamic Distribution of Private Keys over MANETs

Vanesa Daza[1,3]

Departament d'Enginyeria Informàtica i Matemàtiques
Universitat Rovira i Virgili
Tarragona, Spain

Paz Morillo[2,4] and Carla Ràfols[2,5]

Departament Matemàtica Aplicada IV
Universitat Politècnica de Catalunya
Barcelona, Spain

Abstract

Identity-Based cryptography has been proposed in mobile ad-hoc networks (MANETs) to provide security. However, the figure of the Private Key Generator (PKG) is not adequate in the MANET setting, since it may not be reachable by all nodes, can fail during the life-time of the protocol or can even be attacked, compromising the whole system. Previous works distribute the task of the PKG among a set of nodes by means of a secret sharing scheme.
In this paper we propose an efficient solution to emulate in a dynamic and distributed way the role of the PKG in so that even new nodes joining the network are able to issue shares of the master key of an Identity-Based scheme. In this way, the distributed PKG spreads dynamically among the nodes as the network increases. Furthermore, the techniques we propose may be suitable for other protocols over MANETs.

Keywords: mobile ad-hoc networks, ID-based schemes, secret sharing schemes

1 Introduction

A mobile ad-hoc network (also known as MANET) is a self-organized wireless network of mobile nodes without any fixed infrastructure. Therefore, the network topology may change rapidly and unpredictably.

[1] This author is partly supported by the Catalan Government under grant 2005 SGR 00446, and by the Spanish Ministry of Science and Education through project SEG2004-04352-C04-01 "PROPRIETAS".

[2] These authors are supported by Spanish Ministry of Science and Education through project TIC 2003-00866.

[3] Email: vanesa.daza@urv.cat

[4] Email: paz@ma4.upc.edu

[5] Email: crafols@ma4.upc.edu

doi:10.1016/j.entcs.2006.11.008

Security in MANETs is raising a lot of interest, since some of its characteristics, such as lack of infrastructure, absence of a trusted third party or constraints in the communication channel and the mobile devices themselves, (for instance, energy constraints) make it difficult to secure.

Traditional public key infrastructure is hardly implementable in MANETs, since even if the tasks of a Certificate Authority are emulated or distributed by some nodes in the network, the access to the certificates is extremely costly and difficult to guarantee and should include frequent broadcasts of lists of revoked users.

Recent works proposed the use of Identity Based schemes, in which the public key of a user is a well known aspect of its identity and thus the authenticity of public keys is immediately guaranteed. Moreover, revocation can be implemented adding an expiry date to the identity.

However, one of the main drawbacks of using ID-based cryptography in a mobile ad-hoc network is the need of a Private Key Generator (in short, PKG).

We provide an efficient solution to distribute in a dynamic way the role of the PKG by conveniently using a bivariate polynomial to share the master key. Therefore, this construction provides a solution to jointly perform the role of the PKG in a mobile ad-hoc network.

Somehow, our techniques can be seen as a secret sharing scheme without a fixed set of nodes holding shares of a secret. We stress that, in our construction, the secret does not change throughout the life-time of the MANET, independently if new nodes are jointed or not. This point makes our construction especially suitable for dynamically distribute the master key of the Identity-Based Scheme.

Note that in our scheme threshold property is not the goal, but a tool to initialize a MANET with security, decentralized and allowing dynamism.

On top of all the natural features of Identity Based schemes, our proposal also provides a non-interactive pairwise key agreement.

Summing up, with our proposal, we provide an efficient solution of performing a Private Key Generator in a MANET. The whole combination of efficiency, ID-based feature and mobile ad-hoc network scenario have not been proposed before, up to our knowledge.

1.1 Previous Work

Several works [9,10,5] stress suitability of ID-based schemes for securing ad-hoc networks. Authors in [5,10] suggest emulating the public key generator by using a (t, n)-threshold secret sharing scheme in a similar way as in wired networks (see, for example [8]). However this solution lacks of the required dynamism for a mobile ad-hoc network. For example, at least t of the initial nodes that jointly play the role of the public key generator must be reachable throughout the life of the MANET for any new node joining the network.

On the other hand, Saxena *et al.*, in [12], provide a solution that allows new nodes to play the role of share distributors, but at the cost of a very interactive procedure. This is hard to implement in MANETs as for example high energy

consumption is needed for communications.

Actually, since the first proposal relating threshold cryptography and mobile ad-hoc networks [15], threshold secret sharing has been also used in other works for securing ad-hoc networks [6,7] in a dynamic way. Furthermore, they show how to construct threshold signatures in the dynamic scenario of a mobile ad-hoc network, pointing out the possibility of extending their results to other cryptographic actions.

Recently, Saxena *et al.* [13] provide an efficient admission protocol for ad-hoc networks. They make use of similar secret sharing techniques as in our paper, but their goal is to establish a pairwise key in a non-interactive way.

Outline of the paper: The rest of the paper is distributed as follows. Section 2 reviews some basic concepts on ID-based schemes and secret sharing schemes. Our proposal for adapting the role of a PKG to a MANET is detailed in Section 3. Some applications that derive from our construction are described in Section 4. Finally, we conclude in Section 5.

2 Preliminaries

In this section we briefly review some concepts that will be useful in the rest of the paper. We begin by defining ID-based schemes and fixing some notation. Afterwards, we review some basics on secret sharing schemes.

2.1 ID-Based Schemes

In an identity-based encryption scheme, a pair master public key/ private key is generated by the PKG. Once this master key is established, arbitrary identities may be used as public keys for the scheme. When a sender wants to encrypt a message for a recipient with identity ID, he only needs the master public key and the identity ID. In order to decrypt a message, the user ID must obtain the corresponding private key from the PKG.

More formally, an identity-based encryption scheme is specified by four probabilistic polynomial time (PPT) algorithms (see for instance [2]):

- ID.Gen takes a security parameter k and returns the system parameters `ID.pms` and master private key `ID.msk`. The system parameters include the master public key and the description of sets $\mathcal{M}$, $\mathcal{C}$, which denote the set of messages and ciphertexts respectively. `ID.pms` is publicly available, while `ID.msk` is kept secret by the trusted authority.
- ID.Ext takes as inputs `ID.pms`, `ID.msk` and an arbitrary string $ID \in \{0,1\}^*$ and returns a private key d_{ID} to the user with identity ID. This must be done over a secure channel, since d_{ID} enables to decrypt ciphertexts under the identity ID.
- ID.Enc takes as inputs `ID.pms`, $ID \in \{0,1\}^*$ and $M \in \mathcal{M}$. It returns a ciphertext $C \in \mathcal{C}$.
- ID.Dec takes as inputs `ID.pms`, $C \in \mathcal{C}$ and a private key d_{ID}, and it returns $M \in \mathcal{M}$ or rejects.

In this paper we will consider the Identity Based scheme proposed by Boneh and Franklin in 2001 [2]. The system parameters are $params = (q, \mathbb{G}, \mathbb{G}_1, e, P, P_{pub})$ where $\mathbb{G}$, $\mathbb{G}_1$ are groups of the same prime order q, $P_{pub} = sP$ is the master public key, s is the master secret key and e is an admissible pairing. Admissible pairings are maps $e : \mathbb{G} \times \mathbb{G} \to \mathbb{G}_1$ with the following properties:
1. Bilinear: $e(aP, bQ) = e(P, Q)^{ab}$
2. Non-degenerate: $e(P, P) \neq 1_{\mathbb{G}_1}$ for all $P \in \mathbb{G}$
3. Computable: there exists an efficient algorithm to compute $e(P, Q)$ for any $P, Q \in \mathbb{G}$.

2.2 Secret Sharing Schemes

The idea of secret sharing schemes was independently introduced by Shamir [14] and Brickell [3]. Roughly speaking, the problem is to deal pieces, or shares, of a secret among a set of parties so that some coalition of them can jointly reconstruct it.

More formally, a secret sharing scheme is a method by means of which an special figure, called usually *dealer*, shares a secret s among a set $\mathcal{P} = \{P_1, \ldots, P_n\}$ of n parties. Each party P_i is to receive privately from the dealer a piece of information s_i so that s is reconstructible from any set of $t+1$ of the s_i, but no set of less than t of the s_i supplies any information about s. The family of subsets of players that are allowed to recover the secret is called access structure. We refer to this particular case, where sets with more than $t + 1$ players are authorized to recover the secret, as (t, n)- threshold access structures.

Shamir's secret sharing scheme [14] realizes (t, n)-threshold access structures by means of polynomial interpolation. We briefly review it next:

Let $\mathbb{Z}_q$ be a finite field with $q > n$ and let $s \in \mathbb{Z}_q$ be the secret. The dealer picks a polynomial $P(x)$ of degree at most t, where the free term of $P(x)$ is s and all other coefficients are selected from $\mathbb{Z}_q$, uniformly and independently, at random. That is, $P(x)$ has the form:

$$P(x) = \sum_{j=0}^{t} a_j x^j$$

Every party P_i is publicly associated to a field element α_i. Distinct parties are mapped to distinct field elements. The dealer privately sends to party P_i the value $s_i = P(\alpha_i) = \sum_{j=0}^{t} a_j \alpha_i^j$, for $i = 1, \ldots, n$.

Lets see that the scheme realizes a (t, n)-threshold access structure. Let us assume the set of parties willing to recover the secret s is $\{P_1, \ldots, P_{t+1}\}$. The secret s can be obtained from $s_1, \ldots, s_{t+1}$ as $\sum_{i=0}^{t} \lambda_i s_i$, where $\lambda_i = \prod_{j \neq i} \frac{\alpha_j}{\alpha_j - \alpha_i}$ are the Lagrange coefficients.

It is not difficult to prove that any set of less than $t + 1$ parties obtains no information about s, that is, any secret is equally probable given the shares of this set.

A generalization of Shamir secret sharing scheme has also been widely used to distribute points on elliptic curves [2,1]. For our construction we will need to

distribute the private keys in an ID-based scheme, that is private keys of the form sQ_m, where Q_m is a point on the elliptic curve. This is simply realized by sharing s as in the previous paragraph and setting the products s_iQ_m to be the shares of the secret sQ_m. Trivially, this realizes a (t, n) threshold secret sharing scheme, since: $\Sigma\lambda_i s_i Q_m = (\Sigma\lambda_i s_i)Q_m = sQ_m$.

3 Dynamic Distribution of Keys for ID-Based in MANETs

In this section we provide a solution for the distribution of keys for ID-Based in a mobile ad-hoc network. First of all, we describe the scenario we consider in this paper and afterwards, we propose a solution fitting our proposed scenario to provide the corresponding private keys to new nodes joining the MANET.

3.1 Setting up the Scenario

Let $\mathcal{N} = \{N_1, \ldots, N_m\}$ be the set of possible nodes of a mobile ad-hoc network, where m is an upper bound on the possible number of nodes.

Every node has an own unique identity ID, that must be bound to the node for its entire lifetime, non transferable and verifiable. We will note the identity of the node N_i as ID_i. Identities of network nodes could be chosen in different ways. For example, [9] gives some different options to choose the identities of the nodes, distinguishing three cases of nodes an identity is bound to:

- a user operating a network node, i.e. the ID string corresponds to the user, e.g. the user's email address;
- a device, i.e. the ID is bound to the hardware, e.g. the MAC address;
- a network interface, in that case the ID might be derived from the IP address.

We assume that, initially, the MANET is composed by a set of nodes $\mathcal{N}_F = \{N_1, \ldots, N_\ell\}$. These nodes are the *founders* of the MANET. Considering the high probability that they meet each other at the time of MANET foundation, we assume these nodes to be pairwise securely connected. If this is not the case, this fact can be simulated by using some secure routing protocol technique [11].

We consider two different types of nodes. On the one hand, a node that is able to provide shares of the master key. We refer to this kind of node as a *sharing master node* or simply as a *node*. We also consider nodes in the MANET that, although connected to the set of nodes, are not able to provide shares of the master key. We refer to these nodes as *potential nodes*.

Roughly speaking, in our proposal, founder nodes jointly generate shares of the master key s. The way nodes generate this information will be described in detail in Section 3.2. In this way, founder nodes become nodes of the MANET.

The use of the shares is two-fold: on the one hand, they will allow to provide to a new node requiring its secret key, shares of it. On the other hand, if a new node has received enough information from a subset of nodes in $\mathcal{N}_F$, this potential node

becomes a node. With this technique, the set of nodes performing the task of the PKG in a distributed manner spreads over the network dynamically.

We stress that our proposal specially suits the mobility condition of MANETs. Indeed, a potential node may obtain a set of shares of its secret key from a set of nodes. Even if it moves away, connecting in this way to a different set of nodes in the MANET, it can recover its private key after obtaining enough shares from nodes in the MANET.

Due to space constraints, we focus on a *honest-but-curious* scenario. That is, we assume that some set of corrupted nodes (either nodes or potential nodes) get information from honest nodes but perform the protocol correctly. From now on, we assume any set of corrupted nodes has cardinality at most t.

3.2 Dynamic ID-Based Keys in MANETs

Next we describe in detail our protocol. First of all we describe the part where the founder nodes jointly create shares of the master key. Afterwards, we detail the phase where a potential node connected to a node of the MANET requires a share of its secret key to a set of nodes in the MANET. Finally, we show the phase where a potential node turns into a master node after obtaining enough information from a set of master nodes. We refer to these three phases as *Initialization Phase*, *Request and Computational Phase* and *Node Aggregation Phase* respectively.

Initialization Phase This phase is performed only once in the protocol. Founders of the MANET perform it at the beginning of the protocol. We assume the set of founder nodes is $\mathcal{N}_F = \{N_1, \ldots, N_\ell\}$. This part of the protocol basically consists of the joint generation of a random secret value in $\mathbb{Z}_q$. To do so, the idea is that founders jointly set up a (t, ℓ)-threshold secret sharing scheme using bivariate polynomials. Then, shares are univariate polynomials instead of field elements as in [14]. Although this fact increases the complexity of the protocol depending on the chosen parameter t, it is necessary to provide dynamism to the protocols, which is crucial in MANETs because of their inherent mobility and unpredictability.

Note that we are considering the case where $t < \ell$. If this is not the case, some simple solutions can solve this problem. For example, founders can try to increase the set of founder nodes or instead of this decrease the threshold t.

- Every node N_i, for $i = 1, \ldots, \ell$, chooses a random symmetric bivariate polynomial $P^i(x, y)$ in variables x and y with degree at most t in each of them. We write the polynomial as

$$P^i(x, y) = \sum_{k,j=0}^{t} a^i_{k,j} x^k y^j,$$

  where $a^i_{k,j} \in \mathbb{Z}_q$ and $a^i_{k,j} = a^i_{j,k}$ for any $k, j = 0, \ldots, t$.
- Every node N_i, for any $i = 1, \ldots, \ell$, sends to the rest of founder nodes N_j, the univariate polynomial resulting of evaluating $P^i(x, y)$ in $y = h_j$, where

$h_j = h(ID_j)$ for a hash function $h : \{0,1\}^* \to \mathbb{Z}_q$. That is, $P^i(x, h_j)$. We refer to this univariate polynomial as $P^i_j(x)$. Further, we note $P(x,y) = \sum_{i=1}^{\ell} P^i(x,y)$.

- Finally, every node N_i computes

$$S_i(x) = \sum_{j=1}^{\ell} P_i^j(x) = \sum_{j=1}^{\ell} P^j(x, h_i) = P(x, h_i).$$

The jointly generated random secret will be $s = \sum_{i=1}^{\ell} P^i(0,0) = P(0,0)$ and the share of the secret of a node N_i will be the value $s_i = S_i(0) = P(0, h_i)$.

It is not difficult to check that the previous protocol realizes a (t, ℓ)-threshold access structure.

Request and Computational Phase Let N_m be either a master key node or a potential node with identity ID_m willing to obtain the secret key that matches with its public key $Q_m = H(ID_m)$. The secret key will be $d_m = sQ_m$, where s is the secret that has been jointly generated by nodes in $\mathcal{N}_F$ as described before. In order to obtain its secret key, N_m must request a set of master nodes for his secret key. After certain authentication, contacted nodes will provide it with some pieces of information that will allow it to compute its secret key. More specifically:

- N_m selects a group $\widetilde{\mathcal{N}_m}$ of at least $t+1$ nodes from the set of neighbour nodes $\mathcal{N}_m$ is connected with. Without loss of generality, we assume this set of nodes is $\widetilde{\mathcal{N}_m} = \{N_1, \ldots, N_{t+1}\}$.
- N_m requests its share of d_m to every node in $\widetilde{\mathcal{N}_m}$.
- Node N_i, for $i = 1, \ldots, t+1$ sends to N_m the piece of information $Q^i_{priv} = s_i Q_m$.
- N_i is able to compute its secret key d_m as $d_m = \sum_{i=1}^{\ell} \lambda_i Q^i_{priv}$, where the λ_i's are the appropriate Lagrange coefficients.

Remark 1. Note that in case N_m is a founder node, then N_m only needs to interact with a subset of t nodes in order to obtain enough shares to compute its secret key d_m.

Remark 2. If node N_m is connected to a number of nodes less than $t+1$, it can request its secret key d_m to this set of nodes, and after obtaining the corresponding sharing, use its mobility to connect to other different nodes and request for its secret key. In such a way, when N_m has $t+1$ different shares he will be able to get the secret key in the same way as described before. We stress that in this case, the mobile potential node does not have to request to a set of a least $t+1$ nodes, but N_m can re-use previously obtained shares from other nodes.

Node Aggregation Phase Let N_m be either a master node or a potential node with identity ID_m as before. Potential nodes may turn into a master node if they are connected to a set of at least $t+1$ nodes and they request and receive corresponding information from this set.

More specifically the protocol must be realized as follows:

- N_m selects a group $\widetilde{\mathcal{N}_m}$ of at least $t+1$ nodes from the set of nodes $\mathcal{N}_m$ is connected with. Without loss of generality, we assume this set of nodes is

$\widetilde{\mathcal{N}_m} = \{N_1, \ldots, N_{t+1}\}$.

- N_i requests to be accepted as a node.
- Node N_i, for $i = 1, \ldots, t+1$ sends to N_m the piece of information $P(h_i, h_m) = S_i(h_m) = S_m(h_i)$.
- Then, N_m is able to obtain his polynomial share $S_m(x)$ by using Lagrange interpolation:

$$S_m(x) = \sum_{i=1}^{t+1} \prod_{j \neq i} \frac{x - h_j}{h_i - h_j} S_i(h_m) = \sum_{i=1}^{t+1} \prod_{j \neq i} \frac{x - h_j}{h_i - h_j} P(h_i, h_m) = P(x, h_m),$$

and compute its share of the secret s as $s_m = S_m(0)$.

4 Applications

In this section we point out some applications that derive from our construction.

Identity-Based Cryptography As a direct application of our construction, nodes in a MANET can take advantage of the benefits that Identity Based Public Key Cryptography (ID-PKC) entails. For example, the ID-based signature scheme of Cha and Cheon [4]. The problem of revoking users can be addressed by including an expiry date in the identity corresponding to every node.

Threshold cryptography Most of threshold cryptography protocols use Shamir secret sharing as building block. For example, threshold signature schemes combine both secret sharing and digital signature schemes.

We suggest, as alternative, using algebraic properties of bivariate polynomials as a building block for other threshold cryptography protocols over MANETs, rather than the classic Shamir scheme.

Key Agreement The public keys of the nodes allow them to agree on a symmetric key. However, as was noted for example in [9], two nodes share the following private information

$$K1_{mn} = e(d_m, Q_n) = e(d_n, Q_m) = K1_{nm}$$

in a non-interactive way. $K1_{nm}$ can be used as a symmetric key. Recall that $Q_i = H(ID_i)$ and $d_i = sQ_i$.
Saxena *et al.* in [13] suggest using $K2_{nm} = S_m(h_n) = S_n(h_m)$ as common secret key. If the identities of the nodes include some expiry date, since $K1_{nm}$ depends on the identities ID_m, ID_n, $K1_{nm}$ changes for every period, while $K2_{nm}$ remains constant. Thus, a node can be compromised for a period without jeopardizing its communications for future periods.

Verifiability and Traceability Verifiability is easy to implement, since the founder nodes must sign a group key including $P_{pub} = sP$, and after reconstructing its private key d_m, node N_m can easily check whether $e(P_{pub}, Q_m) = e(P, d_m)$.
Traceability can also be implemented with the usual verifiable secret sharing (see for example [13]).

5 Conclusion

In this paper we propose a method to distribute among a set of nodes the role of the private key generator in a mobile ad-hoc network. In such a way that, not only initial sharing holder nodes can provide shares of the master key, but also new nodes joining the network, if certain connection constraints are satisfied.

On top of all the natural features of Identity Based schemes, our proposal also provides a non-interactive pairwise key agreement. Techniques on bivariate polynomials may also apply to other distributed dynamic protocols.

Acknowledgements

We thank Giovanni Di Crescenzo and Javier Herranz for useful suggestions and comments.

References

[1] Baek, J., and Y. Zheng. *Identity-based threshold decryption.* In PKC, volume 2947 of Lecture Notes in Computer Science, pages 262–276. Springer-Verlag, 2004.

[2] Boneh, D., and M. Franklin. *Identity-based encryption from the weil pairing.* In Advances in Cryptology - CRYPTO '2001, volume 2139 of Lecture Notes in Computer Science, pages 213–229. Springer-Verlag, 2001.

[3] Brickell, E.F. *Some ideal secret sharing schemes.* J. Combin. Math. and Combin. Comput., 9:105–113, 1979.

[4] Cha, J.C., and J.H. Cheon. An identity-based signature from gap Diffie-Hellman groups. In *Public Key Cryptography*, volume 2567 of Lecture Notes in Computer Science, pages 18–30, 2003.

[5] Deng, H., A. Mukherjee, and D.P. Agrawal. *Threshold and identity-based key management and authentication for wireless ad hoc networks.* In International Conference on Information Technology: Coding and Computing (ITCC'04), volume 1, pages 107–115, 2004.

[6] Di Crescenzo,G. , G.R. Arce, and R. Ge. *Threshold cryptography for mobile ad hoc networks.* In volume 3352 of Lecture Notes in Computer Science , pages 91–104, 2004.

[7] Di Crescenzo,G., R. Ge, and G.R. Arce. Improved topology assumptions for threshold cryptography in mobile ad hoc networks. In Proceedings of the 3rd ACM workshop on Security of ad hoc and sensor networks, pages 53–62, 2005.

[8] Herranz, J. and G. Sáez . "Distributed key generation for id-based schemes". In Proceedings of VIII Spanish Meeting on Cryptology and Information Security, RECSI'04, pages 215–223, 2004.

[9] Hoeper, K., and G. Gong. *Bootstrapping security in mobile ad hoc networks using identity-based schemes with key revocation.* Technical report, University of Waterloo, Canada, 2006.

[10] Khalili, A., J. Katz, and W.A. Arbaugh. "Toward secure key distribution in truly ad-hoc networks". In Proc. of IEEE Security and Assurance in Ad-Hoc Networks at Int'l Symp. on Applications and the Internet (SAINT'03), volume 22, pages 342–346. IEEE, 2003.

[11] Li, J., Y. Pan, and Y. Xiao. *Performance study of multiple route dynamic source routing protocols for mobile ad hoc networks.* J. Parallel Distrib. Comput., 65(2):169–177, 2005.

[12] Saxena, N., G. Tsudik , and J.H. Yi. Identity-based access control for ad hoc groups. In Proceedings of Information Security and Cryptology, pages 362–379, 2004.

[13] Saxena, N., G. Tsudik , and J.H. Yi. "Efficient node admission for short-lived mobile ad hoc networks". In Proceedings of 13th IEEE International Conference on Network Protocols, pages 269–278, 2005.

[14] Shamir, A. *How to share a secret.* Commun. ACM, 22(11):612–613, 1979.

[15] Zhou, L. and Z.J. Haas. *Securing ad hoc networks.*, 13(6):24–30,1999. IEEE Network.