A Novel Lightweight Multi-Secret Sharing Technique for Mobile Ad-hoc Networks

Georgios Polymerou, Emmanouil A. Panaousis, Eckhard Pfluegel and Christos Politis

Wireless, Multimedia & Networking (WMN) Research Group
Kingston University London
{g.polymerou, e.panaousis, e.pfluegel, c.politis}@kingston.ac.uk

***Abstract*—In this paper, we are concerned with security for Mobile Ad-hoc Networks (MANETs). Due to the decentralized and self-organizing MANET nature, which implies no direct trusted relationships among nodes, threshold secret sharing algorithms can play a key role in solving the problem of single point of failure in the traditional public-key infrastructure (PKI) architecture. We first motivate the need for efficient secret sharing techniques by reviewing security requirements for MANETs with a view of creating a prototype implementation, focusing on threshold cryptographic techniques for key management solutions. With the aim of designing a computationally lightweight secret sharing scheme, we then propose a novel technique for multi-secret sharing that will improve some aspects of the key management.**

***Index Terms*—Mobile Ad-hoc Networks, Threshold Cryptography, ID-Based Cryptography, Key Management, Multi-Secret Sharing**

I. Introduction

A *Mobile Ad-Hoc Network* (MANET) is a wireless communications network that does not rely on any fixed infrastructure. MANETs consist of mobile nodes interconnected by wireless multi-hop communication paths. In such a network, the participating nodes do not need access points to communicate with each other; a node reaches another through intermediate (relay) nodes using a variety of available routing protocols. MANETs are self-configuring, self-maintaining, adaptive and with an extremely dynamic topology, since nodes can join or abandon the network at any time. All the above-mentioned characteristics make MANETs complex, with multiple parameters to be taken into account, in order to implement an efficient network. Nevertheless, in the past few years, there have been many applications, both civilian and military, that take advantage of the unique concept of MANETs. Thus, like in any kind of communications network, security is a primary concern.

A great number of authors have investigated aspects, requirements and solutions for MANET security - see for example [1], [2], [3] and the references therein. The task of creating solutions for providing the standard security goals of confidentiality, integrity and availability is particularly challenging for MANETs, primarily for the following reasons:

- *Exposure through wireless medium*: MANETs impose several challenges since the use of wireless links allows a large set of attacks to target these networks. This happens because signals are propagated from the source over the open air to all directions and prospective attacks can be launched by anyone and from any direction.
- *Weaknesses of routing protocol*: MANET nodes need to cooperate with each other to carry out routing functionalities. Thus, routing can introduce security holes in the presence of malicious nodes.
- *Lack of fixed or centralized infrastructure*: MANETs do not deploy any fixed infrastructure and there are no actual central nodes to direct packets or enforce a centralized key management technique.
- *Restricted resources*: This may be critical in mobile appliances such as smart phones or tablets due to their resource-constrained nature. This requires lightweight algorithms and data management.
- *Mobility and changing topology*: This MANET's characteristic makes the establishments and maintenance of trust harder.

II. Background

A. The Need for MANET Key Management

Encryption is an important cryptographic tool in computer security, and it is one of the techniques used to address the above-mentioned security issues in MANETs. Conventional cryptographic systems can be divided into symmetric and asymmetric ones, depending on the way they use the keys. Symmetric cryptography involves the use of a single, secret shared key, while asymmetric cryptography involves the use of two different keys (private and public keys). Although symmetric encryption techniques generally require less processing power than asymmetric ones, they entail a number of severe drawbacks when used for MANETs [4]. On the other hand, asymmetric techniques commonly require the existence of a trusted entity to issue certificates and ensure that the public keys belong to a key management authority. This is difficult to achieve in MANETs, and this is the reason why more specialized key management systems have been devised for these networks.

In a cryptographic system in general, providing *key management* is to implement functionality that allows the generation, storage, sharing, use and replacement of keys. Key management in MANETs must, in addition, be able to cope with dynamic topology that is self-organised and decentralised [1].

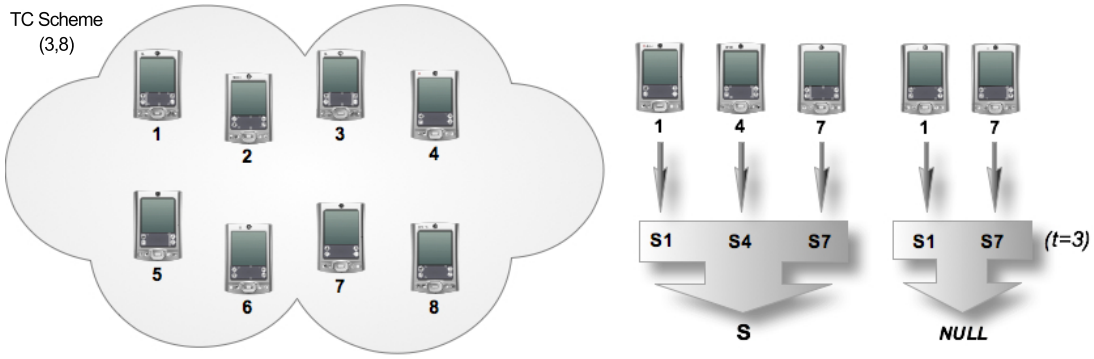

Fig. 1. The concept of threshold cryptography.

A variety of key management schemes can be found in the literature [5]. The seminal paper [6] suggests using threshold cryptography in order to create a distributed public/private key system. Later, the concept of Identity-based cryptography was developed which simplifies the key management process and reduces memory storage cost. We briefly review these concepts in the next section, before we explain their combined use for modern MANET key management.

B. Threshold and Identity-Based Cryptography

The main idea of *Threshold Cryptography* (TC) is to enhance trust by distributing it among a set of n entities, which are called *shareholders*. A TC scheme makes it possible for n shareholders to share the ability to perform a cryptographic operation (i.e. encryption/decryption, digital signing etc.). Additionally, there is a *threshold* value $t \leq n$ associated with the scheme with the property that any number $k \geq t$ of the n parties can execute the desired cryptographic operation, but fewer than t parties will not be able to do this by themselves [7]. Such solutions are referred to as (t, n) *TC schemes*.

Let us consider a secret S in n different shares S_i,($i \leq n$), so that the knowledge of at least t shares is required and sufficient to recover the initial secret S (see Fig. 1). Threshold models can be divided into *single secret sharing threshold* e.g. Shamirs t-over-n scheme based on Lagranges interpolation, and *threshold sharing functions*, such as geometric based threshold. These schemes are being used to implement threshold variants of RSA, El Gamal and Diffie-Hellman cryptographic algorithms [8]. By nature, TC schemes are ideal tools for MANETs where the individual nodes of the network are the shareholders of the scheme, and single nodes cannot be trusted.

Shamir was the first to introduce the concept of *Identity-Based Cryptography* (IBC) [9]. The idea in IBC is that each user which wants to establish a security association (SA) with another user, can generate the latters public key based on publicly available identity information (for example, an IP address, email etc.), while the private key is generated by a trusted third party (TTP), called *private key generator*. This approach of key management is simpler and has reduced memory storage cost compared to conventional public key techniques. Consequentially, it lends itself well to the use within a MANET key management.

Fig. 2 represents a generic ID-Based scheme, in which Node A uses the public key of node B (ID_B) and the public key of the PKG (K^+_{PKG}) to cipher a message M. Then, Node B, in order to decrypt the cipher text, uses its private key (K^-_B), received from the PKG.

C. Threshold & ID-based Combination for Key Management in MANETs

The concepts of TC and IBC have been combined in order to form a variety of key management schemes for MANETs [10], [4], [11], [12], [13], [9]. The concepts of TC and IBC have been combined in order to propose a variety of key management schemes that are adequately efficient for MANETs [10]. In the following, we discuss the most important of these schemes found in the literature.

The Identity-based key management (IKM) presented in [4], uses the above mentioned combination, where each node's public and private key are generated by a node-specific ID-Based element and a network-wide common element. IKM involves three phases: key predistribution (during the network initialization), key revocation (in order to minimize the damage from compromised nodes), and key update (keys updates in periodic intervals or when the number of revoked nodes reaches a predefined value).

The scheme proposed in [11] consists of two operations: distributed key generation (providing the networks master key and the key pair for each node) and identity-based authentication (providing end-to-end authentication and confidentiality). Here, all network's nodes form a distributed PKG set. Thus, each node, in order to obtain its private key must contact at least t nodes of the PKG; each PKG node generates a secret part of that private key and sends it back to the requesting node.

The self-organised identity-based authentication and key exchange (IDAKE) in [12], involves symmetric cryptography and pairing-based keys specified in six functions: setup, extract, distribute, shared key computation, key renewal, and key revocation. All these functions are performed by the network

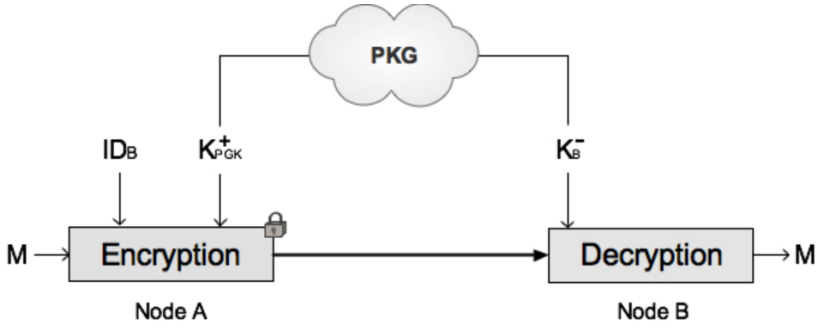

Fig. 2. The concept of Identity-based cryptography.

nodes themselves, without any external PKG, which has been replaced by a t-over-n TC scheme.

Finally according to the key management scheme proposed in [13], all of the nodes form a distributed PKG set like [11], called threshold PKG, which has a master private key distributed in a t-over-n TC scheme. The nodes' public keys are their identities, while their private keys must be computed by the nodes of the threshold PKG. The scheme assumes that identities are recorded in hardware and cannot be altered.

Despite the fact that some of the above-mentioned techniques establish TC and IBC based certificateless public-key management schemes for MANETs, many issues remain to be resolved. First of all, due to the nature of TC, the security of the entire network is breached when a threshold number of nodes-shareholders are compromised. In addition, updating keys requires each node to individually contact a threshold number of shareholders, which causes a significant communication overhead in a large scale MANET. Moreover, all schemes using IBC suffer from the fact that the private key of each node is computed and hence known by PKG.

Last but not least, ID-based schemes lack anonymity and privacy preservation, as public keys are directly derived from the identity of the participating nodes. All the following aspects contribute to the overall performance of a security solution for MANETs:

- The efficiency of the cryptographic techniques;
- The secret sharing method;
- The traffic required for maintaining the key management.

D. Secret Sharing

Secret sharing is at the heart of any asymmetric key-management system that is based on threshold cryptography. There are three main techniques for secret sharing: Shamirs scheme [14] based on polynomial interpolation, Blakleys secret sharing based on solving linear systems [14] and an approach based on the Chinese Remainder Theorem [15]. An overwhelming number of additional secret sharing schemes exist in the literature [16], which refine or improve various aspects that might arise in different scenarios.

Multi-secret sharing (or also referred to as *multiple secret sharing*) is concerned with the continuous sending of different secrets, by updating shares correspondingly. It can also be used for sharing large secrets, as they can be divided into several smaller secrets and be shared using multi-secret sharing. Usually, this is implemented using particular online secret sharing methods.

For the application we are planning to implement, a specific type of secret sharing (*online secret sharing*), will be particular useful. In online secret sharing [17], apart from the shares that are distributed amongst the players, additional information is "*posted on a bulletin board*". Effectively, this information is published in an authentic manner but without the need for confidentiality. Online secret sharing is useful for MANETs due to it can replace the need for encrypting the above additional information and securely distribute it among MANET nodes.

E. Our Contribution

In this paper, we focus on providing a secret sharing approach that minimizes the size of shares as much as possible. We will inspire ourselves from recent work based on multi-sharing and matrix-projection [18], [6], [19] in order to find an alternative method that offers certain advantages.

We will further explore the multi-secret sharing aspect with the vision to apply our proposed method in a particular cluster-based architecture for MANETs such as the one proposed in [20]. 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.

III. Proposed Method

As part of a TC scheme, employed within a MANET key-management system, one needs to address the method used for secret sharing. In this paper, we propose an online multi-secret sharing method, which in terms of reducing the share size, is comparable with [18], [6]. Due to its lightweight nature, we expect higher performance than standard secret sharing technique, once implemented.

Let us consider a secret s, to be distributed into n different shares s_i $(1 \leq i \leq n)$, so that the knowledge of at least t $(1 < t \leq n)$ shares is required and sufficient to recover the initial secret s.

Similarly as in [18], we convert the given secret scalar value s into a square matrix S of dimension $t \times t$ by choosing a suitable prime number $p < s$, write s as a number with

Algorithm 1 Sharing Secret s.

1: Choose suitable prime number $p < s$, and compute the digits of s as a number to the base p.
2: Convert the secret s into a $t \times t$ matrix S by using these digits.
3: Compute similarity transformation T, that results in the companion matrix $C = T \cdot S \cdot T^{-1}$.
4: Encrypt and share the t coefficients of f, with n MANET nodes, by using any existing (t, n) TC scheme.

Algorithm 2 Reconstructing Secret s.

1: Reconstruct the characteristic polynomial f and the value of p by acquiring at least t shares.
2: Build C from the t coefficients of f.
3: Compute S from C, by using the public transformation T as $S = T^{-1} \cdot C \cdot T$.
4: Reconstruct s from S and p.

base p, retrieve its digits and populate the matrix S with these values. Here, we choose p so that we obtain t^2 digits.

Using basic linear algebra techniques, a similarity transformation T can be computed that results in a new matrix C of a special form, the so-called *companion form*. All entries of C are zeros except for the elements in the upper off-diagonal which are ones, and the bottom row, as follows:

$$C = \begin{pmatrix} 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & 1 & \ddots & \vdots \\ \vdots & & \ddots & \ddots & 0 \\ 0 & 0 & \dots & 0 & 1 \\ c_0 & c_1 & \dots & c_{t-2} & c_{t-1} \end{pmatrix}. \quad (1)$$

The elements in this bottom row are known to be related to the *coefficients of the characteristic polynomial* of the matrix

$$f(\lambda) = -c_0 - c_1 \cdot \lambda - c_2 \cdot \lambda^2 - \dots - c_{t-1} \cdot \lambda^{t-1} + \lambda^t. \quad (2)$$

We now proceed as follows: by using any efficient (t, n) secret sharing scheme, we share the coefficients of f and the value of p, and store the similarity transformation T as public information. In [17] this is referred to as "posting on a bulletin board" (the sharing of such information could be done by broadcasting T throughout the MANET). In this way, we have reduced the initial size s of the secret to $\sum_{i=0}^{t-1} c_i + p$. This value is significantly less than s since it only requires t base p digits (rather than t^2).

It is worth emphasising 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 T. To enable such functionalities, we could for instance use a pre-shared key which is only used for the initial distribution of the shares.

Shareholders are able to reconstruct f, C, p and finally restore the initial secret s, as they know the similarity transformation T.

In order to illustrate our method, we give an example, based on the matrix

$$S = \begin{pmatrix} 2 & 3 & 1 \\ 5 & 4 & 6 \\ 8 & 9 & 7 \end{pmatrix}. \quad (3)$$

of [21]. We hence assume that Step 1 and Step 2 of Algorithm 1 have already been executed, and set for example $p = 19$. For Step 3, we set $u = (0\ 0\ 1)$, $v = uS = (8\ 9\ 7)$, and $w = vS = (3\ 9\ 16)$. The transformation matrix T is derived by putting the vectors $u,\ v,\ w$ as rows:

$$T = \begin{pmatrix} 0 & 0 & 1 \\ 8 & 9 & 7 \\ 3 & 9 & 16 \end{pmatrix}. \quad (4)$$

We now compute $C = T \cdot S \cdot T^{-1}$, this yields the matrix

$$C = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 8 & 13 \end{pmatrix}, \quad (5)$$

which is in companion form.
It is now sufficient to share the secret polynomial

$$\begin{aligned} f &= -c_0 - c_1 \cdot \lambda - c_2 \cdot \lambda^2 + \lambda^3 \\ &= -8\lambda - 13\lambda^2 + \lambda^3 \end{aligned} \quad (6)$$

together with the value of $p = 19$, and the public information T.

IV. Conclusion

In this paper, we have presented a novel approach for multi-secret sharing, based on linear algebra techniques. Our method is in the process of being analysed in terms of computational complexity, and evaluated be means of implementation, so as to be comparable with previous work such as [18], [6]. Furthermore, we intend to intergrate our method in a network simulator, for MANETs, published in our previous work [20]. Our goal will be to confirm that the reduction of the shares' sizes, as proposed in this paper, improves the overall efficiency of the MANET communications, in terms of security. Another aspect of our research will be the detailed comparison of our solution against the method proposed in [6].

We take a bottom-up approach by designing and implementing various components that are reasonably modular so that they can be used for higher-level tasks. They will form an important ingredient of our planned MANET implementation, in a similar way as the matrix-projection method is used for routing in [19].

In the past, we have designed a fundamental system with a basic security mechanism using symmetric key encryption and pre-configured keys [20]. The work described in this paper can enhance this system by improving the overall security

functionalities. In this way, we will propose a novel security framework, for MANETs, with the following advantages:

- Decrease the risk of compromising a network-wide key by distributing cryptographic material to more than one nodes;
- Decrease the computational effort, introduced by previous work as [6], by applying our secret sharing method;

Our future work, within the realm of MANETs, must deem the particular demands of such networks. Therefore, our method will likely to be extended by introducing the following techniques:

- *Dynamic secret sharing*: Here, the number of shares may increase or decrease dynamically during the lifetime of the system. This is particularly important for a MANET, where nodes can join and leave in an unpredictable manner;
- *Proactive secret sharing*: In order to prevent an attacker from collecting shares and reconstruct secret S during a certain duration, we must periodically update the shares without changing the secret. This occurs as the combination of shares from different update phases does not allow deriving the secret. Such a technique is also referred as *share refreshing*.
- *Verifiable secret sharing*: This technique addresses 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.

Another key area of research is concerned with the optimisation of the traffic required to maintain an efficient and robust key management scheme across a MANET. Crucially, *share updating* creates traffic between nodes of the network, which needs to be kept to an acceptable level. The traffic overhead generated by key management in a multi hop network, has been investigated in [22].

REFERENCES

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

[2] L. Zhou and Z. Haas, "Securing ad hoc networks," *IEEE Network*, vol. 13, no. 6, pp. 24–30, Nov./Dec. 1999.

[3] 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. 38–47, Feb. 2004.

[4] Y. Zhang, W. Liu, W. Lou, and Y. Fang, "Securing mobile ad hoc networks with certificateless public keys," *IEEE Transactions on Dependable and Secure Computing*, vol. 3, no. 4, pp. 386 –399, Oct.-Dec 2006.

[5] J. Van Der Merwe, D. Dawoud, and S. McDonald, "A survey on peer-to-peer key management for mobile ad hoc networks," *ACM Computing Surveys*, vol. 39, no. 1, pp. 1–45, 2007.

[6] L. Bai and X. Zou, "A proactive secret sharing scheme in matrix projection method," *International Journal of Security and Networks, Inderscience*, vol. 4, no. 4, pp. 201–209, 2009.

[7] L. Ertaul and N. Chavan, "Security of ad hoc networks and threshold cryptography," *in Proc. International Conference on Wireless Networks, Communications and Mobile Computing*, vol. 1, pp. 69–74, Jun. 2005.

[8] Y. Desmedt, "Some recent research aspects of threshold cryptography," *in Proc. First International Workshop on Information Security (ISW), Springer-Verlag*, pp. 158–173, 1998.

[9] A. Shamir, "Identity-based cryptosystems and signature schemes," *Advances in Cryptology, Springer Berlin / Heidelberg*, vol. 196, pp. 47–53, 1985.

[10] E. da Silva, A. dos Santos, L. Albini, and M. Lima, "Identity-based key management in mobile ad hoc networks: techniques and applications," *IEEE Wireless Communications*, vol. 15, no. 5, pp. 46 –52, Oct. 2008.

[11] A. Khalili, J. Katz, and W. Arbaugh, "Toward secure key distribution in truly ad-hoc networks," *in Proc. Symposium on Applications and the Internet Workshops*, pp. 342–346, Jan. 2003.

[12] H. Deng, A. Mukherjee, and D. Agrawal, "Threshold and identity-based key management and authentication for wireless ad hoc networks," *in Proc. International Conference on Information Technology: Coding and Computing (ITCC)*, vol. 1, pp. 107–111, Apr. 2004.

[13] K. Hoeper and G. Gong, "Bootstrapping security in mobile ad hoc networks using identity-based schemes with key revocation," *tech. rep., Centre for Applied Cryptographic Research, Univ. of Waterloo*, 2006.

[14] A. Shamir, "How to share a secret," *Communications of the ACM*, vol. 22, no. 11, pp. 612–613, 1979.

[15] S. Sarkar, B. Kisku, S. Misra, and M. Obaidat, "Chinese remainder theorem-based rsa-threshold cryptography in manet using verifiable secret sharing scheme," *in Proc. IEEE International Conference on Wireless and Mobile Computing, Networking and Communications (WIMOB)*, pp. 258–262, 2009.

[16] A. Beimel, "Secret-sharing schemes: a survey," *Coding and Cryptology, Springer*, pp. 11–46, 2011.

[17] C. Cachin, "On-line secret sharing," *Cryptography and Coding, Springer*, pp. 190–198, 1995.

[18] K. Wang, X. Zou, and Y. Sui, "A multiple secret sharing scheme based on matrix projection," *in Proc. Annual IEEE International Computer Software and Applications Conference (COMPSAC)*, vol. 1, pp. 400–405, Jul. 2009.

[19] C. Chandrasekar and L. Baboo, "Proactive bais secret sharing scheme for aomdv routing protocol for secured communication in manet," *International Journal of Engineering Research and Applications (IJERA)*, vol. 2, pp. 655–659, Mar.-Apr. 2012.

[20] G. Millar, E. Panaousis, and C. Politis, "Distributed hash tables for peer-to-peer mobile ad-hoc networks with security extensions," *Journal of Networks, Special Issue: Recent Advances in Information Networking, Services and Security*, vol. 7, no. 2, pp. 288–299, Feb. 2012.

[21] L. Bai, "A strong ramp secret sharing scheme using matrix projection," *in Proc. International Symposium on World of Wireless, Mobile and Multimedia Networks (WOWMOM), IEEE Computer Society*, pp. 652–656, 2006.

[22] N. B. Shah, K. V. Rashmi, and K. Ramchandran, "Secret share dissemination across a network," *CoRR*, vol. abs/1207.0120, 2012.