IEICE TRANS. INF. & SYST., VOL.E93–D, NO.7 JULY 2010

PAPER

Ubiquitous and Secure Certificate Service for Wireless Ad Hoc Network

Meng GE[†a)], ***Student Member***, **Kwok-Yan LAM**[†], **Jianbin LI**[††], ***and*** **Siu-Leung CHUNG**[†††], ***Nonmembers***

SUMMARY Wireless ad hoc network is one of the most suitable platforms for providing communication services to support mobile applications in public areas where no fixed communication infrastructure exists. However, due to the open nature of wireless links and lack of security infrastructure in an ad hoc network environment, applications operating on ad hoc network platforms are subjected to non-trivial security challenges. Asymmetric key management, which is widely adopted to be an effective basis for security services in an open network environment, typically plays a crucial role in meeting the security requirements of such applications. In this paper, we propose a secure asymmetric key management scheme, the Ubiquitous and Secure Certificate Service (USCS), which is based on a variant of the Distributed Certificate Authority (DCA) - the Fully Distributed Certificate Authority (FDCA). Similar to FDCA, USCS introduces the presence of 1-hop neighbors which hold shares of DCA's private signature key, and can collaborate to issue certificates, thereby providing asymmetric key management service. Both USCS and FDCA aim to achieve higher availability than the basic DCA scheme; however, USCS is more secure than FDCA in that the former achieves high availability by distributing existing shares to new members, rather than generating new shares as the FDCA scheme does. In order to realise the high availability potential of USCS, a share selection algorithm is also proposed. Experimental results demonstrated that USCS is a more secure approach of the DCA scheme in that it can achieve stronger security than FDCA while attaining high availability similar to that of FDCA. Experiments also showed that USCS incurs only moderate communication overheads.

key words: *security, availability, ad hoc networks, key management, certificate authority*

1. Introduction

As wireless handheld devices have become more popular, it is desirable to provide a ubiquitous communication platform for supporting resource sharing, instant messaging, or mobile social networking applications in public areas. Wireless ad hoc network, which consists of mobile nodes connected by wireless links in an ad hoc manner, is one of the most suitable platforms for meeting such communication needs, since it can be self-organized and function without relying on any communication infrastructure to implement the network functions or any authority to manage and control the network [1].

The unique features of wireless ad hoc network, e.g. open nature of wireless links, limited resources of nodes, multi-hop relay and lack of centralized administration etc., may aggravate security and privacy issues of the applications in wireless ad hoc network environment. Asymmetric key management, which almost invariably serves as a basis of security services in a network environment, plays a crucial role in securing the wireless ad hoc network-based applications. However, existing key management schemes for conventional wired networks, e.g. Public Key Infrastructure (PKI) with centralized Certificate Authority (CA) etc., are not suitable for wireless ad hoc network since centralized authority cannot be ensured in a typical ad hoc network due to the single point of failure problem. Providing key management service for ad hoc networks has gained a lot of attention from the research community in the past few years.

The Distributed Certificate Authority (DCA), based on the notion threshold secret sharing, has been a most widely adopted approach to key management for wireless ad hoc networks [2]–[4] since it was proposed in 1999 by [2]. The basic components of a DCA consist of a trusted dealer and a number of server nodes (or called DCA members). The trusted dealer is a trusted entity which is responsible for selecting system parameters such as threshold values, computing shares of the CA's private signature key based on the threshold scheme, and securely distributing them to the members before deploying the system. The members collaborate to issue certificates as long as at least a threshold number of them are available. However, previously proposed DCA schemes such as those presented in [2]–[4] suffer from the availability problem when operating in a wireless ad hoc network where network partitioning occurs frequently. In such case, a threshold number of members might only be available intermittently in some (or even all) segments, so the availability of the DCA could be interrupted. More importantly, since most of the operations of DCA needs to communicate with at least a threshold number of members, which typically are many hops away, communication overheads and delay are considerable.

A variant of DCA, i.e. the Fully Distributed Certificate Authority (FDCA), was proposed by [5], [6]. The FDCA scheme aims to improve availability of DCA and to reduce communication delay by means of *local service*, i.e. distributing shares of the CA's private signature key to almost all the neighbors of a joining node (requestor) and making each well-behaving node a DCA member, thereby improving the availability and efficiency of the key management service. The main drawback of FDCA is the weak security protection of CA's private signature key. This is because wireless ad hoc network is highly heterogeneous from the perspective of security protection of nodes. In other words, in a typical deployment scenario, some nodes are better pro-

Manuscript received October 9, 2009.

[†]The authors are with Tsighua University, Beijing, China.
[††]The author is with Academia Sinica, China.
[†††]The author is with The Open University of Hong Kong, China.
a) E-mail: gem04@mails.tsignghua.edu.cn

DOI: 10.1587/transinf.E93.D.1848

tected than others, and there are nodes which are more vulnerable to attacks. Since the security of system is always determined by the weakest point(s) of the system, the FDCA scheme which distributes shares to almost all nodes is inherently subjected to serious security problems.

Another kind of schemes were proposed in [7]–[9]. In these schemes, security authority such as CA is not required. Instead, each node independently issues certificates to others and utilizes certificate chain consists of certificates issued by others to authenticate a public key. The schemes of this kind adapt to the self-organized nature of wireless ad hoc network in that they could be initialized spontaneously without a trusted dealer. However, they have the following disadvantages when the scale of the networks becomes larger: 1) the efficiency problem, i.e. one has to verify more than one certificate to authenticate a public key, and 2) the security problem, i.e. as the length of the chain increases, the trustworthiness of the public key obtained will be decreased. For the sake of limited space, we do not recap all existing schemes in this paper. Please refer to [10] for a complete survey.

In this paper, we propose the Ubiquitous and Secure Certificate Service (USCS) based on the FDCA scheme. As with FDCA, the authoritative power of CA, i.e. the power to issue, update or revoke certificates, is distributed to all the well-behaving nodes based on a threshold scheme. A quorum of DCA members within 1-hop scope of the certificate requester could collaborate to issue a certificate. However, the proposed scheme differs from FDCA in that the security issues from which FDCA suffers, i.e. compromising any threshold number of nodes will break the system is addressed. The basic idea of USCS is to distribute existing shares to new DCA members instead of generating new shares for them. Suppose there are totally m DCA members in the network and (n, t) threshold scheme is used, the main differentiation of FDCA and the proposed protocol could be highlighted as follows:

- In FDCA, a new DCA member is always distributed with a new share. As a result, there are as many different shares as DCA members, i.e. m different shares in total.
- In USCS, a new DCA member is distributed with one of the n existing shares, i.e. there are n different shares in total, no matter how many DCA members exist. In this case, even if the attacker successfully compromised t nodes, he might not be able to obtain t shares.

By reducing the number of non-duplicated shares in the system, the proposed scheme can efficiently improve the security of the key management service. While improving the security, duplicated shares may also reduce the availability of the key management service. In order to maintain the availability, we further design a share selection algorithm for the USCS scheme. Through analysis and simulation, we illustrate that USCS with appropriate parameters not only can address the security issue, but also have availability very close to FDCA and moderate communication overhead in our scenario.

This paper is organized as follows: we present the system models as the basis of our scheme in Sect. 2. Details of the USCS scheme are proposed in Sect. 3. We analyze the security property of USCS in Sect. 4. The performance of proposed scheme is evaluated the simulation results are analyzed in Sect. 5. Finally, we conclude our work in Sect. 6.

2. System Models

Before presenting the USCS scheme, we will discuss the system models of USCS in this section, which captures aspects of its system environments.

2.1 Network Model

According to the mobility characteristics of mobile nodes, we classify wireless ad hoc networks into two basic types:

- Stable wireless ad hoc network. In networks of this kind, frequent movements of nodes are uncommon. In most of the time, locations of nodes are kept fixed. Practical examples includes wireless ad hoc networks deployed for a temporary conference or mobile social applications based on wireless ad hoc networks on a train [11]. Note that although it is stable in terms of node mobility, the membership of the wireless ad hoc network could be dynamic due to nodes' join and leave.
- Dynamic wireless ad hoc network. It denotes the type of wireless ad hoc networks where the nodes are typically moving freely and frequently. The popular Vehicular Ad hoc Networks (VANET) [12] and wireless ad hoc networks deployed for the emergency response operations [13] fall into this category.

In this paper, we will focus on the former type and take mobile social application on a train as a practical application scenario.

2.2 Node Classification

According to the functionality, network nodes in our system could be classified into three types:

- DCA member. The DCA member is node which has legal credential or can be verified by its neighbors. It is trustworthy enough to provide key management service according to application-specific policies. A DCA member will not only be issued with a certificate indicating its node type, but also obtain a share of DCA's private signature key, whereby providing the key management service.
- Non-DCA member. Non-DCA member is node which has legal credential or can be verified by its neighbors, while it is not trustworthy enough to be a DCA member. For example, if it ever exhibited some suspicious behaviors, the node may not be accepted as a DCA member. Although it will not provide key management

service directly, it could be a user of the key management service.
- External node. A node which is not verifiable to its neighbors cannot be accepted as any of above two types. Thus, neither certificate nor share will be issued for nodes of this kind. Without a legal certificate, it will be excluded from the system.

In practice, mobile nodes in wireless ad hoc networks are heterogeneous in terms of the communication capability. For example, different handheld devices usually have different radio ranges. For sake of simplicity, we assume that each node in wireless ad hoc networks has identical range.

2.3 Attack Model

As in other DCA schemes, the main security concern of the USCS scheme is fabrication of certificate. Consider a DCA built based on (n, t) threshold scheme, to fabricate certificates, the attacker has to obtain DCA's signature private key s or at least t shares of s. To obtain a share, the attacker has to compromise the node holding that share. When a node is *compromised*, any resource of the node is under the control of the attacker, including the public/private key pair of the node and the share of s. If there are no more than $t-1$ nodes in the system are compromised, the basic property of threshold scheme [14] could ensure that s cannot be reconstructed or the valid signature cannot be signed. As with other DCA schemes, the proposed scheme is safe, i.e. can defend against certificate fabrication in such a case. In this paper, we further consider the case where the attacker successfully compromises t nodes. In a wireless ad hoc network environment, two kinds of attacks could be launched: 1) selective targets attack, i.e. the attacker compromises any t nodes needed in order to break the system. 2) weakest targets attack, i.e. the attacker compromises the weakest t nodes in order to break the system. On the one hand, it is not difficult to show that any DCA schemes, including the basic DCA scheme, the FDCA scheme or the USCS scheme, can be easily broken under the selective targets attack. On the other hand, due to the heterogeneity of nodes' security, e.g. nodes are heterogenous in terms of physical protection, software or administration vulnerabilities etc., the selective targets attack is much difficult than the weakest targets attack. Thus, we mainly consider the weakest target attack when analyzing the security property of the proposed scheme.

In this paper, each node with legal credential is assumed to be well-behaving, i.e. be able to be a DCA member, unless it exhibits suspicious behaviors. We assume that there is some misbehavior detection mechanism which can recognize and identify the compromised nodes after they exhibit misbehavior. The study of misbehavior detection mechanism in wireless ad hoc networks is beyond the scope of this paper.

3. The USCS Scheme

The USCS scheme is a variant of DCA schemes, which aims to improve the security of FDCA while maintain its availability. In this section, we firstly present basic idea of the USCS scheme which distributes existing shares instead of generating new ones to new DCA members. In order to address the availability issues caused by duplicated shares, we further propose a share selection algorithm. Then we present the USCS protocol which considers not only security aspect, but also availability of the system.

3.1 The Basic Idea

The main goal of USCS is to address the security issue from which the FDCA scheme suffers. In the FDCA scheme, when a new DCA member is joining the system, its *1-hop neighbors* will collaborate to generate a new share of DCA's private signature key for the new member. As a result, there are as many shares as members in the system. A basic security policy of the FDCA scheme is that almost all nodes are DCA members except the ones exhibited malicious behaviors. In this connection, compromising t weakest nodes in system may obtain the DCA private signature key and break the key management system. In the proposed scheme, our basic idea is to distribute an existing share rather than to generate a new share for a new DCA member, thus reducing the total number of (non-duplicated) shares. When a new node is joining the system as a DCA member, its 1-hop neighbors will collaborate to choose a share from existing ones for the new node. Then the selected share is distributed to the new node securely. The details of the USCS scheme (e.g. how to distribute the selected share to the new node securely) will be presented in Sect. 3.3. Although we adopt similar security policy of the FDCA scheme, i.e. almost all nodes are treated as DCA members except the ones exhibited malicious behaviors, the total number of (non-duplicated) shares in USCS-based system is effectively reduced. Therefore, the probability of breaking the system by compromising t weakest nodes will largely reduced and the security of system is improved (as shown in Sect. 4). The reduced number of shares not only improve the security of system, but may simplify some key operations needed by the DCA or FDCA scheme. For example, it avoids the collaborative share generation of FDCA scheme. Besides, since there are much less shares in the USCS scheme, the share updating operation of the FDCA scheme may also be largely simplified. Based on this idea, we proposed the basic USCS scheme in [15].

3.2 The Share Selection Algorithm

Although the basic scheme can effectively reduce the total number of shares, it might suffer from the availability problem because of duplicated shares. A basic property of threshold scheme using Shamir's secret sharing [14] is that only different (non-duplicated) shares could be used to reconstruct the secret or provide the distributed service. Since a DCA member is distributed with an existing share, there might be a lot of duplicated shares in the system. In such a case, when one node is joining the DCA, it might not get

the certificate service even if there are sufficient number of DCA members in its 1-hop scope. In other words, the distribution of shares on one's 1-hop neighbors largely affect the availability of the key management service.

In this section, we enhance availability of the basic scheme in stable wireless ad hoc networks by optimizing the share distribution. Since nodes in stable wireless ad hoc networks will not move around frequently in most cases, the distribution of shares is relatively stable. Share distribution in stable wireless ad hoc networks largely depends on the way we select the shares.

To study the share selection mechanism, we firstly define the concept "*overlapping part* of two nodes" as the part overlapped by radio range of two nodes. Similarly, the overlapping part could be defined for a number of nodes. With the definition of overlapping part, there are four basic properties as follows.

Property 1: There exists an overlapping part for one node and any of its 1-hop neighbors.

Property 2: There exists an overlapping part of any two 1-hop neighbors of one node.

Property 3: There exists an overlapping part of one node and its 2-hop neighbors.

Property 4: The overlapping part of one node and any of its 1-hop neighbors is larger than the overlapping part of the node and any of its 2-hop neighbors in size.

Property 1 and 2 are straightforward to be proven. Property 3 could be easily deduced from Property 2 since from the angle of the 1-hop neighbor, other two nodes are its neighbors respectively. Due to space constraints, we do not provide the details of the proof for Property 1, 2 and 3. Property 4 could be proved informally as follows. Let r denote the radius of node's radio range, the size of overlapping part of two neighbors where one node is just next to the edge of another one's radio range could be represented as $\frac{2}{3}\pi r^2 - \frac{\sqrt{3}}{2}r^2$. The fact that two nodes are 1-hop neighbors indicates that they are in the radio range of each other. Therefore, the size of overlapping part of two 1-hop neighbors falls in $(\frac{2}{3}\pi r^2 - \frac{\sqrt{3}}{2}r^2, \pi r^2)$; while the size of overlapping part of two 2-hop neighbors falls in $(0, \frac{2}{3}\pi r^2 - \frac{\sqrt{3}}{2}r^2)$. Thus we have Property 4.

Based on the notion of overlapping part, another concept *Full Function Part (FFP)* is defined as the overlapping part formed by DCA members with at least t different shares. In a FFP, one could get certificate service from its 1-hop neighbors successfully since there are t non-duplicated shares. Suppose that $(10, 3)$ threshold scheme is utilized and members v_1, v_2, v_3 hold three non-duplicated shares s_1, s_2, s_3 respectively, an example of FFP is illustrated in Fig. 1, where the gray part denotes a FFP.

Wireless ad hoc networks could be divided into FFP and non-FFP. By definition of FFP, any node can only get the certificate service in the FFP. Although it is impractical to manipulate the overlapping parts, which mainly depend on the topological position of nodes, the distribution of shares could be controlled by the share selection procedure, whereby affecting the size of the FFP. Ideally, in order to increase availability, shares should be selected/distributed in order to maximize the current FFP in size. In this connection, the principle of share selection algorithm is straightforward, i.e. each time to select a share, the FFP should be extended as much as possible so that for a new node to join, it is more likely to fall into the FFP and get certificate service from its 1-hop neighbors.

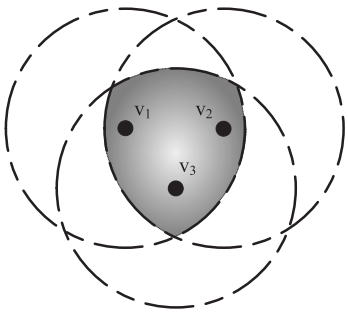

Fig. 1 An example of FFP formed by three DCA members.

According to Properties 1 and 3, two nodes within 2-hop scope will always form overlapping part. However, 2-hop neighbors will always have overlapping part smaller than the nodes which are 1-hop neighbors according to Property 4. Therefore, we argue that 2-hop neighbors might be less important than 1-hop neighbors, which is verified by our simulation results (as shown in Sect. 5).

An important parameter h is defined for the share selection algorithm. h denotes how many hops we consider when selecting a share for a new DCA member. For example, if $h = 0$, it means that the share selection algorithm does not consider distribution of shares on any other nodes. If $h = 1$, it means that the procedure only consider distribution of shares on requester's 1-hop neighbors; while $h = 2$ means both 1-hop and 2-hop neighbors are considered.

Let v_r denote the joining node and v_i denote any of its 1-hop neighbors. Suppose that v_i has just received a request from v_r, the share selection algorithm could be described as follows:

If $h = 2$, v_i has to collect the share distribution information from v_r's 1-hop and 2-hop neighbors. v_i will firstly send its node ID and share ID as well as its neighbor list NL_i to v_r. Upon receiving the message, v_r generates its own neighbor list NL_r. Then v_r broadcasts NL_r and other received neighbor lists to its 1-hop neighbors. NL_r and other neighbor lists contains all necessary information about v_r's 1-hop and 2-hop neighbors. With these lists, a decision table could then be generated, which tell the rough distribution of shares around v_r. An illustration of the decision table is shown in Fig. 2. Note that it may include a lot of duplicated nodes in the neighbor lists, but each node should be counted only once. With the decision table, the share s_k is selected as:

$$\min_{1 \le i \le n} \{\alpha n_i + \beta n_i'\}$$

Share ID of s_i (SID_i)	Number of neighbors with s_i (n_i)	Number of 2-hop neighbors with s_i (n'_i)
SID_1	…	…
SID_2	…	…
…	…	…
SID_n	…	…

Fig. 2 The decision table.

where n_i is the number of neighbors with share s_i, n'_i is the number of 2-hop neighbors with share s_i. Both the values could be easily evaluated from the decision table. α and β are weight values. According to Property 4, $\alpha > \beta$, i.e. $\alpha : \beta > 1$ should hold. The estimation of $\alpha : \beta$ is further analyzed in Sect. 5 by simulation.

If $h = 1$, v_i will only send its node ID and share ID to v_r. With the share IDs, v_r will generate its own neighbor list NL_r. Then v_r broadcasts NL_r to its 1-hop neighbors. Upon receiving NL_r, v_i will convert NL_r to a decision table as shown in Fig. 2 and select the share s_k as

$$\min_{1 \le i \le n} \{n_i\}$$

If $h = 0$, v_i will directly evaluate the selected share ID for v_r based on v_r's node ID as

$$SID_k = H(v_r) \quad k \in [1 \dots n]$$

where $H()$ is a hash function. Given that all users use the same hash function, the neighbors will agree on the same share ID SID_k.

3.3 The USCS Protocol

In this section, we present the USCS protocol based on the share selection algorithm. Before describing the details of the proposed protocol, the used symbols are defined.

- $v_i, (i = 1, 2, \dots, m)$: any node in the system and its node ID. The set of all nodes is denoted by V.
- v_r: the joining node and its ID.
- C_r: the certificate of v_r.
- pC_r^i: the partial certificate issued by v_i for v_r.
- $s_k, (k = 1, 2, \dots, n)$: any share in the system. The share ID of s_k is denoted by SID_k.
- V_k: the set of the nodes which hold s_k.
- N_{v_r}: the set of DCA members in v_r's 1-hop scope.
- PK_r: the public key of node v_r.
- PR_r: the private key of node v_r.
- D_r: the credentials of v_r, which are used for registering to (be verified by) nodes in N_{v_r}.
- $E_r()$: the encryption algorithm using PK_r as public key.
- $S_r()$: the digital signing algorithm using PR_r as signature private key.
- NL_r: the neighbor list of v_r, which includes node ID and share ID of nodes in N_{v_r}.

The USCS protocol is presented as follows.

Step 1 When one node v_r is to join the system, it requests its neighbors N_{v_r} for a certificate C_r. The request includes the credential D_r.

Step 2 Upon receiving the request, the neighbor v_i verifies D_r according to application-specific policies. According to verification result of the credential and trustworthiness of v_r, v_i will act as follows:

- If v_r is accepted as a DCA member candidate (as stated in Sect. 2.2), the share selection algorithm will be launched.
- If v_r is accepted as a non-DCA member candidate, the partial certificate for v_r will be sent along with C_i to v_r directly. C_i is used by v_r to obtain PK_i and verify the signature of v_i.
- Otherwise, v_i exits the protocol immediately.

If v_r is accepted as a DCA member candidate, v_i will act as follows according to the system parameter h:

- If $h = 0$, v_i will select an existing share ID as $SID_k = H(v_r) \quad k \in [1 \dots n]$ and issue a partial certificate including SID_k for v_r.
- Else if $h = 1$, v_i will reply to v_r with v_i, SID_i, which are signed by PR_i.
- Else if $h = 2$, v_i will reply to v_r with v_i, SID_i and NL_i, which are signed by PR_i.

Note that C_i is included in each kind of reply, so that v_r can obtain PK_i and verify v_i's signature.

Step 3 Upon receiving the replies, v_r will verify the signatures and act as follows.

- If it is accepted as a non-DCA member or $h = 0$, the protocol will go to Step 5 directly.
- Else if it is accepted as a DCA member and $h = 1$, v_r will generate NL_r using the received share IDs. Then v_r will broadcast NL_r and $E_r(NL_r)$ to N_{v_r}.
- Else if it is accepted as a DCA member and $h = 2$, v_r will generate NL_r using the received share IDs. Then v_r will broadcast NL_r as well as received neighbor lists to N_{v_r}. The signatures of neighbor lists are sent as well.

Note that since a neighbor list entry typically consists of only the neighbor's node ID and corresponding share ID, which is about several of bytes in size, even the neighbor list(s) is broadcasted in 1-hop scope, it will not incur heavy communication overhead.

Step 4 Upon receiving the broadcast, v_i checks the validity of the received neighbor list(s) by verifying the attached signature(s). If the verification is passed, v_i will select the share based on the decision table (as stated in Sect. 3.2). Then v_i will issue a partial certificate for v_r including the selected share ID. Otherwise, v_r will be marked as suspicious node.

Step 5 If there are no less than t partial certificates, C_r could be generated by combining the partial ones. If v_r is

Table 1 The USCS protocol, $h = 2$, v_r is a DCA member.

The USCS protocol
$v_r \rightarrow \forall v_i \in N_{v_r} : v_r, PK_r, D_i$
$v_i \rightarrow v_r : v_i, SID_i, NL_i, S_i(NL_i), C_i$
$v_r \rightarrow \forall v_i \in N_{v_r} : NL_r, S_r(NL_r), \{NL_i, S_i(NL_i) \mid v_i \in N_{v_r}\}$
$v_i \rightarrow v_r : pC_r^i$
$v_r \rightarrow \forall v_j \in V : C_r$
$v_j \in V_k \rightarrow v_r : E_r(s_k)$

accepted as a DCA member and s_k is selected, it will flood a notification including C_r to inform the selection of share and request s_k from any DCA member holding that share.

Step 6 Upon receiving the notification, SID_k will be recorded by each node v_j, if v_j holds s_k, it will encrypt s_k as $E_r(s_k)$ and send $E_r(s_k)$ to v_r.

In Step 1 and 2, a joining node use credential to register to its 1-hop neighbors. The credentials could be internal certificates which could be verified by nodes of some other organizations. Besides, the registration could be performed in an Out-of-Band manner, e.g. by physical contact and infrared channel [16]. The design of the registration process is outside the scope of this paper, In most cases, DCA members hold the given share can be found in several hops. Even if there is no DCA member with the selected share in the network, any t of its neighbors could generate the given share. We refer readers to [5] for the share generation process. To defend against the tampering and replaying attack, the signing data, time stamp and nonce should be attached for each message. For clarity of the exposition, however, we do not explicitly show these information in the description. Given that $h = 2$ and the requester is a candidate of DCA member, the proposed protocol could be illustrated as Table 1.

4. Security Analysis

Wireless ad hoc network is highly heterogeneous from the perspective of security protection of the network nodes. This is because, in a typical deployment scenario, some nodes are better protected than others, and there are nodes which are more vulnerable to attacks. As the security of a system is always determined by the weakest point of the system, the FDCA scheme which distributes shares to almost all nodes is inherently subjected to more serious security problems.

We consider the weakest targets attack model in which the attacker compromises the weakest targets, i.e. the weakest nodes in terms of physical protection, software or administration vulnerabilities. Given a (n, t) threshold scheme, we evaluate the security of the system by the metric *break-in probability*, which is the probability of the system being broken when the attacker compromised t weakest nodes. For FDCA, the system will be broken if any t DCA members are compromised. Thus, the probability is 100%. For USCS, even if the attacker manage to compromise t weakest DCA members, it may not be able to obtain t different (non-duplicated) shares, hence is unable to break the system.

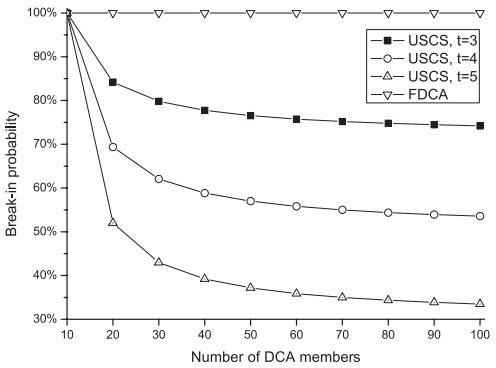

Fig. 3 Security analysis.

Suppose that (n, t) threshold scheme is used, and the shares are distributed evenly to m DCA members, i.e. each share is distributed to about $(\frac{m}{n})$ nodes, then the break-in probability could be computed as:

$$P = \frac{C_n^t \cdot (\frac{m}{n})^t}{C_m^t}$$

Figure 3 shows that the break-in probability could be effectively reduced by properly setting the threshold parameters n and t. With a fixed n and threshold value t, the probability is reduced as the number of DCA members m increases. For example, given that $n = 10$ and $t = 5$, the probability is reduced from 100% to 33.5% as m grows from 10 to 100. This is because more DCA members will produce more duplicated shares in the USCS scheme. Therefore, the key management service will be more secure when the system/network become larger. With a fixed n and number of DCA members m, the probability is also reduced as the threshold value t increases. Given that $n = 10$ and $m = 100$, the break-in probability is reduced to about 74.2%, 53.6% and 33.5% when t is set to 3, 4 and 5 respectively. By selecting proper threshold parameters, the security of the system (the break-in probability) could be adjusted in a flexible manner.

A malicious requester might try to manipulate the share selection procedure by revising or even fabricating neighbor list(s). Since each neighbor list is signed by its owner (in Step 2), either revising or fabricating the neighbor list(s) could be easily detected.

Note that there is another technical challenge in the USCS scheme. To prevent a malicious node from obtaining more than one shares through making repeated requests, the history information of share distribution should be recorded when the notification is flooded (in Step 5). With the history information, malicious requests could be effectively detected. Distributed Hash Tables (DHT) approaches for wireless ad hoc network [17] could be used for facilitating and optimizing the operations.

5. Experiment

In this section, we will discuss and evaluate some impor-

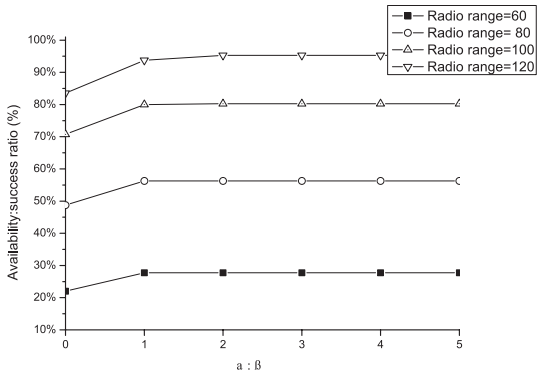

Fig. 4 Chosen of $\alpha : \beta$ ($t = 4$).

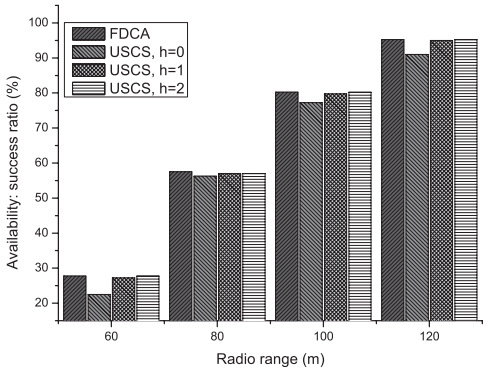

Fig. 5 The comparison of availability ($t = 4$).

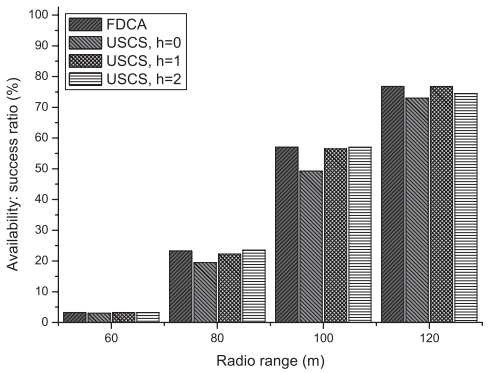

Fig. 6 The comparison of availability ($t = 5$).

tant aspects of the performance of USCS, e.g. the availability and communication overheads etc. In particular, USCS schemes with different parameter settings as well as the FDCA scheme are implemented as agents respectively on Network Simulator 2 (NS2).

We consider a typical scenario on the train, i.e. a series of scenarios with size 550 m × 3.3 m are generated, where 50 nodes (simulating the passengers and users of the communication platform) are location-fixed in most of the time. At the beginning of each scenario, only 10 of the 50 nodes are activated, each of which hold a non-duplicated share. Other nodes become activated and request to join our system one after another every 20 second.

Before comparing the performance of USCS and FDCA, we firstly discuss the choice of α and β, which denotes the weights of 1-hop and 2-hop neighbors respectively. The availability of USCS with $h = 2$ versus radio range of nodes is illustrated as Fig. 4, where the rate of α to β is set to 0, 1, 2, 3, 4, 5, and $(10, 4)$ threshold scheme is employed.

Figure 4 shows that in our scenarios, the availability of the proposed scheme is not sensitive to the rate of α and β when $\alpha > \beta$. The result also verifies the validity of Property 4, i.e. the 1-hop neighbors might be more important than the 2-hop ones when both 1-hop and 2-hop neighbors are considered. In the following discussion, the rate of α and β will be set to 4:1 as a fixed parameter.

USCS with different parameters are compared with FDCA in terms of availability. In order to compare the availability under various scenarios, different threshold parameters and radio ranges, which may significantly affect the availability, are considered. In particular, we adopted the $(10, 4)$ and $(10, 5)$ threshold schemes, and the radio range are chosen as 60 m, 80 m, 100 m, 120 m respectively.

In Fig. 5 and 6, the availability of the schemes is evaluated by the *success ratio* of certificate request, which measures the number of successful certificate requests over the total number of requests.

Figure 5 and 6 show that the success ratio always increases as the radio range increases from 60 m to 120 m in each scheme. It is also shown that setting a larger threshold value t will result in lower availability. This is because in a system with a larger t, more DCA members are required to provide the service.

In each scenario, FDCA exhibits higher success ratio than USCS with $h = 0$. This is because in USCS with $h = 0$, when a new DCA member is joining the system, its share is selected randomly from existing ones regardless of the share distribution nearby (as stated in Sect. 3.2). Therefore, more duplicated shares may exist in a certain area and the availability of system may be weaken. By employing share selection algorithm and setting the parameter h to 1 or 2, the availability of USCS can be improved. As illustrated in Fig. 5 and 6, the availability of USCS with $h = 1$ and $h = 2$ is very close to the FDCA scheme.

Since the overlapping part of nodes in 1-hop scope is always larger than the overlapping part of nodes in 2-hop scope (as stated in Property 4), nodes which are 2-hop away may contribute less to the formation of FFP. In other words, 2-hop neighbors are less important than 1-hop neighbors in the share selection procedure. Therefore, although the availability of USCS with $h = 1$ is slightly less than the availability of USCS with $h = 2$ in some cases, they are very close with each other in most cases.

One exception is that the availability of USCS with $h = 1$ is higher than the availability of USCS with $h = 2$ when the threshold value is set to 5 and radio range is set to 120 m. This may partially because in the latter case, where the radio range and threshold value is both large, the increase communication overheads brought by the USCS pro-

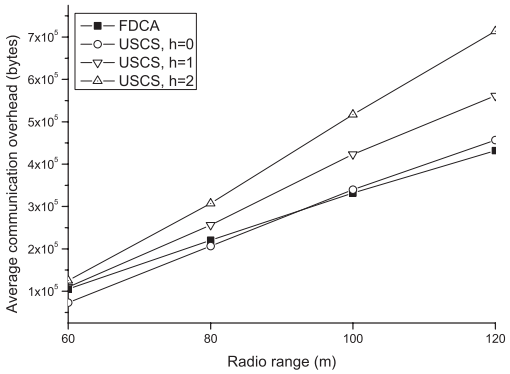

Fig. 7 The comparison of communication overheads ($t = 4$).

tocol will incur more interferences, which counteract the improvement of availability brought by share selection.

In addition to the availability, communication overheads of USCS and FDCA are evaluated and compared as well. The communication overheads measure the overall packets brought by the key management service in bytes. Although USCS avoids the share generation procedure which is necessary in FDCA, it needs to collect the information of share distribution from neighbors of the requester. Therefore, the communication overheads of USCS are largely decided by the parameter h. Comparisons of the communication overheads of USCS with different h and FDCA are illustrated as Fig. 7.

As shown in Fig. 7, the communication overheads of FDCA and USCS with $h = 0$ are similar. The communication overheads of USCS with $h = 1$ and $h = 2$ are heavier than FDCA or USCS with $h = 0$. Although the availability is very close, the overheads of USCS with $h = 1$ is much less than the one with $h = 2$. Figure 7 also shows that as the radio range becomes larger, the communication overheads of USCS increase faster than the FDCA scheme. This may partially because we simply employed a flooding mechanism in Step 5 without any optimization.

When $h = 0$, USCS incurs light communication overhead, while it cannot achieve high availability as FDCA does. When $h = 2$, USCS achieves high availability very close to FDCA, while it brings much heavier communication overheads. In our scenario, USCS with $h = 1$ achieves both high availability and moderate communication overheads.

6. Conclusion

In this paper, we proposed a secure asymmetric key management scheme, i.e. USCS for wireless ad hoc networks. By distributing existing shares rather than generating new shares, total number of non-duplicated share is efficiently reduced in USCS. Therefore, it is more secure against the weakest targets attack from which FDCA suffers. USCS with different system parameter h are further studied based on simulation. We learned from the simulation results that with different h, USCS exhibits different performance in terms of availability and communication overhead. It is illustrated by the analysis and experiment result that with appropriate parameters setting, USCS not only can address the security issue, but also has availability very close to FDCA and incurs only moderate communication overhead in our scenario.

References

[1] C. Perkins, Ad hoc networking, Addison-Wesley, Reading, MA, 2001.
[2] L.D. Zhou and J.H. Zygmunt, "Securing ad hoc networks," IEEE Netw., vol.13, no.6, pp.24–30, 1999.
[3] S. Yi, and R. Kravets, "MOCA: Mobile certificate authority for wireless ad hoc networks," 2nd Annual PKI Research Workshop (PKI 2003), NIST, pp.65–79, Gaithersburg MD, USA, 2003.
[4] J. Luo, J.P. Hubaux, and P.T. Eugster, "DICTATE: DIstributed certification authority with probabilisTic frEshness for ad hoc networks," IEEE Trans. Dependable and Secure Computing, vol.2, no.4, pp.311–323, 2005.
[5] J. Kong, P. Zerfos, H. Luo, S. Lu, and L. Zhang, "Providing robust and ubiquitous security support for mobile ad-hoc networks," IEEE 9th International Conference on Network Protocols, pp.251–260, Riverside, CA, 2001.
[6] H.Y. Luo, J.J. Kong, P. Zerfos, S.W. Lu, and L.X. Zhang, "URSA: Ubiquitous and robust access control for mobile ad hoc networks," IEEE/ACM Trans. Netw., vol.12, no.6, pp.1049–1063, 2004.
[7] S. Capkun, L. Buttyan, and J. Hubaux, "Self organized public-key management for mobile ad hoc networks," IEEE Trans. Mobile Comput., vol.2, no.1, pp.52–64, 2003.
[8] R.D. Li, J. Li, P. Liu, and H.H. Chen, "On-demand public-key management for mobile ad hoc networks," Wireless Commun. Mobile Comput., vol.6, no.3, pp.295–306, 2006.
[9] S. Capkun, J.P. Hubaux, and L. Buttyan, "Mobility helps peer-to-peer security," IEEE Trans. Mobile Comput., vol.5, no.1, pp.43–51, 2006.
[10] 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.3–45, 2007.
[11] K. Farkas, L. Ruf, M. May, and B. Plattner, "Framework for service provisioning in Mobile ad hoc networks," First International Conference on Telecommunications and Computer Networks, San Sebastian, Spain, 2004.
[12] M. Raya and J.P. Hubaux, "Securing vehicular ad hoc networks," J. Computer Security, vol.15, no.1, pp.39–68, 2007.
[13] M. Ge, K.Y. Lam, D. Gollmann, S.L. Chung, C.C. Chang, and J.B. Li, "A robust certification service for highly dynamic MANET in emergency tasks," Int. J. Commun. Syst., vol.22, no.9, pp.1177–1197, 2009.
[14] A. Shamir, "How to share a secret," Commun. ACM, vol.22, pp.612–613, 1979.
[15] M. Ge and K.Y. Lam, "Ubiquitous and secure certificate service for mobile ad hoc network," the 5th IEEE/IFIP International Conference on Embedded and Ubiquitous Computing, pp.312–317, 2008.
[16] D. Balfanz, D. Smetters, P. Stewart, and H. Wong, "Talking to strangers: Authentication in ad-hoc wireless networks," 9th Annual Network and Distributed System Security Symposium, San Diego, CA, 2002.
[17] F. Araujo, L. Rodrigues, J. Kaiser, C. Liu, and C. Mitidieri, "CHR: A distributed hash table for wireless ad hoc networks," 25th IEEE International Conference on Distributed Computing Systems Workshops, pp.407–413, 2005.

Meng Ge received his BS degree in computer science from the Shandong University, China, 2004. He is currently working toward the PhD degree in the key laboratory for information system security, ministry of education, Tsinghua University, Beijing, China. His research interests include security in mobile ad hoc networks, social networks and security management. He is a student member of the IEEE.

Kwok-Yan Lam is the Director of Key Laboratory for Information System Security, Ministry of Education, PR China. He has been a Professor at the School of Software, Tsinghua University, PR China since 2002. Prior to joining the Tsinghua University, Professor Lam has been a faculty member of the National University of Singapore and the University of London since 1990. His main research interests include distributed systems, information security and tamper-resistant design. Professor Lam was a visiting scientist at the Isaac Newton Institute of the Cambridge University and a visiting professor at the European Institute for Systems Security. He has been a chief security architect for a number of electronic banking and electronic government systems in Singapore and Hong Kong. Professor Lam received his B.Sc. (First Class Honours) from the University of London in 1987 and his Ph.D. from the University of Cambridge in 1990.

Jianbin Li is a Senior Engineer of the Information Centre, State Administration of Taxation, P.R. China. He is a Visiting Professor of the School of Software, Tsinghua University; and a Visiting Researcher of the Software Institute, Academia Sinica. He specializes in design and planning of very large scale networks and information security management. His research interests include information security management, security risk analysis and disaster recovery planning.

Siu-Leung Chung is an Associate Professor at the School of Business and Administration, The Open University of Hong Kong. Prior to joining The Open University, he has been a faculty member of the National University of Singapore and the University of Toledo, Ohio, USA since 1991. His main research interests are information and system security, e-commerce security and software project management modeling. Dr. Chung received his B.Sc. (Engineering) from the University of Hong Kong in 1977 and his Ph.D. in Computer Science from the University of Illinois in 1991.