EURASIP Journal on Wireless Communications and Networking
a SpringerOpen Journal

REVIEW Open Access

A survey and taxonomy of distributed certificate authorities in mobile ad hoc networks

Mohammad Masdari[1*], Sam Jabbehdari[2], Mohammad Reza Ahmadi[3], Seyyed Mohsen Hashemi[1], Jamshid Bagherzadeh[4] and Ahmad Khadem-Zadeh[3]

Abstract

Certificate authorities (CAs) are the main components of PKI that enable us for providing basic security services in wired networks and Internet. But, we cannot use centralized CAs, in mobile ad hoc networks (MANETs). So, many efforts have been made to adapt CA to the special characteristics of MANETs and new concepts such as distributed CAs (DCAs) have been proposed that distribute the functionality of CA between MANET nodes. In this article, we study various proposed DCA schemes for MANET and then classify these schemes according to their internal structures and techniques. Finally, we propose the characteristics of an ideal DCA system that can be used to verify the completeness of any DCA scheme. This classification and taxonomy identify the weakness and constraints of each scheme, and are very important for designing more secure, scalable, and high performance DCA systems for MANETs and other networks.

Keywords: distributed certificate authority, threshold cryptography, registration authority (RA), PDCA, CA nodes, cluster head, communication overhead, OLSR protocol, encryption, digital signature

1.Introduction

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

The simplest approach to implement a CA is to assign CA task to single node. One of the main problems of this approach is its availability and it can bring the entire MANET to a halt if it moves out of the MANET. Furthermore, it acts as a single point of failure if it is compromised by an attacker. A replicated CAs can be used to solve availability problem of previous scheme [1]. Therefore, using x replica, the system can withstand (x - 1) failures because the CA service is available as long as there is at least one operational CA. But, this approach creates consistency problems when CA nodes cannot find each others. Also, if any CA node is compromised, we will have several points of compromise in MANET. To solve all of these problems, we must use distributed certificate authority (DCA). The rest of the article is organized as follows: In Section 2, DCAs in MANET are discussed. In Section 3, the threshold cryptography is described and in Section 4, we classify and compare various proposed DCA schemes. At last, in Section 5, we present the properties of an ideal DCA system for MANET.

2. Distributed CA

A DCA is realized through the distribution of the CA's private key to a number of shareholding DCA nodes. However, the public key of the DCA will be known by all network's nodes and will be used to verify signatures of certificates issued by the DCA. When operations such as issuing or revoking certificates are required, a

* Correspondence: m.masdari@iaurmia.ac.ir
[1]Science and Research Branch, Computer Engineering Department, Islamic Azad University, Tehran, Iran
Full list of author information is available at the end of the article

threshold of available shareholding DCA nodes should participate [2]. In Table 1, we compare the properties of centralized (none replicated) CA with distributed CA systems. It shows that although distribution increases reliability and availability, it decreases the security of system.

Zhou et al. [3] present a fault-tolerant and secure online certification authority system for local area network and internet, called COCA which cannot be used in MANET environment.

The DCA approach has also been proposed in Wireless Mesh and Vehicular Networks and a number of schemes have been devised for these. Since a little work has been done in Wireless Mesh Networks, only one scheme has been proposed. In MANET, many DCAs schemes have been designed and they can be classified as partially or fully distributed certificate authorities (FDCA). In partially implemented DCA (PDCA), services of the CA are distributed to a set of specialized server nodes using secret sharing. Each of these nodes can generate partial certificates and a client can create a valid certificate by combining enough number of these partial certificates. In this case, these special server nodes must have high energy and the inherent heterogeneity of the nodes in network is utilized to choose the candidates for CA nodes. However, if all the nodes in MANET were identical, the nodes of the distributed CA might be chosen randomly.

One of the advantages of PDCA is its practicality and generality. It has some disadvantages as follow:

- **Availability problem:**

  The most important risk of PDCA is the network partitioning. Therefore, if a threshold number of DCA nodes are not available in the network segments, we will have availability problem.

- **Performance problem:**

  Server nodes may be scattered all around the network and may be many hops away. Therefore, communication delay will be increased proportional to the number of hopes between client and the server nodes.

- **Number of server nodes:**

  Selecting the right number of nodes for PDCA is not an easy task and we cannot specify the exact number of them. They should be a function of the network size, the degree of resilience required against attacks and number of operations that DCA supports. It is obvious that choosing small number of server nodes for DCA causes bottleneck and creates performance problems.

Table 1 Comparison of centralized CA and distributed CA

	Centralized CA	Distributed CA
Security	High	Low
Availability	Low	High
Fault tolerance	Low	High
Messaging overhead	Low	High
Performance	High	Low
Message exchange	Low	High
Scalability	High	Low
Routing dependent	No	Some schemes
Special nodes	Required	Only PDCA
User nodes mobility	High	Some scheme
DCA nodes mobility	Low	High
Revocation source	Owner issuer	Owner, issuer, k accusation
Validity of certificate	High	Low
Messaging complexity	One request, one reply	K Request, K Reply

In FDCA, services of a CA are distributed to all nodes and using secret sharing, each of these nodes can generate partial certificates [4]. FDCA reduces the communication delay and improves the availability because almost all the neighbors of a requesting node hold shares of the DCA's private signature key. However, it allows attackers break the system more easily and when an intruder enters the network and compromises one or more nodes, he becomes as good as a valid one. To overcome this problem, an intrusion detection system is required to be presented in the network, which can identify the misbehaving or compromised nodes, and remove them from the network. In some schemes such as [5], certificates have limited lifetime and after expiration time they are revoked. Thus, compromised keys cannot be used anymore. The amount of this expiration time will be a tradeoff between security and performance.

Regarding the large amount of expiration time, security weakens and with the small amount of expiration times, certificates must be frequently renewed, so this may produce performance problems, because large amount of data must be transferred between DCAs and client nodes. To solve performance problems, the expiration time of well-behaved nodes can be increased. In Table 2, we have compared the properties of PDCA and FDCA. In all FDCA and PDCA schemes, the communication pattern between a client and DCA nodes is one-to-many and many-to-one, which means that a client needs to contact at least k CA nodes and receive at least k replies. The simplest form of communication between clients and CA nodes is flooding. Although this

Table 2 Comparison of PDCA and FDCA

	PDCA	FDCA
Client to DCA communication	One-to-many	One-to-many
DCA to client communication	Many to one	Many to one
Security	Higher than FDCA	Low
Availability	Lower than FDCA	High
Fault tolerance	Lower than FDCA	High
Mobility support	Low	High
Secret update	Multicast	Broadcast
Client distance from DCA	One hop or more	One hop
Network size	Large networks	Small networks
Scalability	High	Low
Special nodes	Required	Not Required
IDS or additional monitoring	Not required	Required

Table 3 Acronyms and abbreviations

Acronym	Expansion
RA	Registration authority
CA	Certificate authority
CCA	Centralized certificate authority
DCA	Distributed certificate authority
PDCA	Partially distributed certificate authority
FDCA	Fully distributed certificate authority
SDCA	Self-initialized DCA
CREQ	Certificate request
CREP	Certificate response
OCSP	Online certificate status protocol
CRL	Certificate revocation lists
CH	Cluster head

approach is effective, it generates a large amount of traffic. Furthermore, it is possible that more than k, CA node receive the certificate request and respond to it; so, a client receives more responses than it needs. Since, almost all of DCA schemes use threshold cryptography we must describe it prior to examining the proposed schemes in detail.

In Figure 1, we have classified all CAs from distribution perspective and it helps us to understand the degree of distribution in each kind of CA.

In this article, Table 3 lists the abbreviations used for DCA systems.

3. Threshold cryptography

In threshold cryptography, operations like the generation of digital signatures are divided among network nodes, so that the action can be done if at least a certain number of parties collaborate. It tolerates the crashes of some components, for example, a $(t - 1,n)$ threshold signature allows, in a group of a total of n parties, any t parties sign jointly, but no coalition of up to $t - 1$ parties can. Any service provided by CA is performed jointly by t ($t \geq 2$) CA nodes, where t is called the threshold of the secret sharing. In this way, even if an attacker has discovered the secret shares of some but less than t CA nodes, the attacker still cannot recover CA's secret key. However, the above threshold secret sharing scheme still fails when the shares of more than t, CA nodes have been discovered by the intruders over a sufficiently long period. To enhance security, secret share update has been proposed, in which a new set of shares are computed after a certain time interval. Therefore, an attacker has to complete the attack within this interval [6]. However, distributing CA on a number of nodes provides some problems:

- First, a user node has to find t, CA server nodes in MANET that is more difficult to find than finding one CA node. Schemes such as flooding for finding CA will not work since they consume too much network resource.
- Second, although efficient update of the secret shares in all CA nodes is not trivial, some schemes have been proposed.
- Third, it is difficult to select right set of nodes to collectively provide the CA services.
- Fourth, it is difficult to provide efficient communication between the mobile nodes and the CA nodes, even in dynamic networks with possible compromises or temporary network partitions [7].

In (k, n) threshold cryptography, k can be chosen between 1 (a single CA for network) and n (FDCA). Setting k to a higher value has the effect of making the system more secure against possible adversaries. But, a higher k value can cause more communication overhead. Thus, the threshold k should be chosen to balance the two conflicting requirements. It is clear that no value will fit all systems, so some approaches such as MOCA provide guidelines for choosing the right value for k.

Threshold cryptography is vulnerable to Sybil attacks, thus some schemes have been presented to solve this

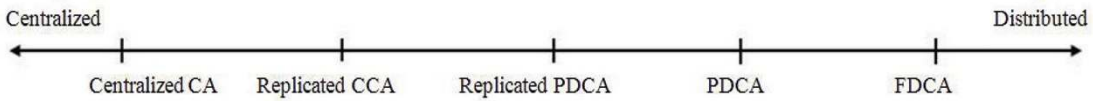

Figure 1 The spectrum of distribution in CAs.

problem. Finally, with any threshold cryptography-based DCA we will have these parameters:

- Total number of nodes in the network (M).
- The number of nodes deputed with CA responsibility (n).
- The minimum number of nodes for signature construction (k).

3.1. Proactive secret sharing

Having enough time, an attacker could compromise k shareholders and this allows him to reconstruct the secret. To defend against such attackers, proactive secret sharing scheme updates the shares periodically, without changing the associated private key of DCA. It can be performed more than refreshing the private key. So, an attacker must compromise k shareholders between the updates. Because shares before and after the refresh operation have no relation and if one share is leaked, it will become useless after the refresh. Determining the periods of private key and key shares' updates is very important and has direct impact on the security and performance of the DCA. Thus, if we choose too long values for these periods, the performance of DCA increases, but the security decreases. Also, if we choose short values for these periods, we may have performance problems. Many messages must be sent for these updates so the security increases and keys change sooner than an attacker can find them. As a result, update periods are functions of performance, security, and the situations of MANET.

4. Classification and taxonomy

In this section, we classify the various proposed PDCA and FDCA schemes into six categories. Two of these categories use existing MANET infrastructure and protocols:

- **Cluster-based DCAs:**

These schemes achieve greater scalability and provide better performance. Also some of them support mobility of DCA nodes.

- **Routing-based DCAs:**

These schemes depend on the special multicast or unicast (proactive or reactive) routing protocols for intra DCA or node to DCA communications.

Although, some of the presented schemes do not depend on any MANET components, they try to solve some of the DCA problems in MANET. These schemes are as follows:

- Self-initialized schemes
- Mobility aware schemes
- Security-based schemes
- Performance and availability-based schemes

In Figure 2, we have classified all of the CA schemes that are proposed for various networks. This taxonomy is very helpful to find out the networks in which DCA systems are used and the techniques that DCA applies.

4.1. Cluster-based DCA

Flat ad hoc networks have poor scalability and the throughput of these networks will decline rapidly with the increase of network nodes. The solution for this problem is *clustering*. The use of clustering in DCAs has two advantages. First, it reduces the storage requirements of individual node, as each node needs to store at most the certificates of the other nodes in the same cluster rather than the entire network.

Second, it reduces the communication overhead and increases the efficiency of certificate management, as certificates are always available to each node at a local repository, few hops away.

Chaddoud et al. [2] proposed a DCA for near-term digital radio (NTDR) cluster-based ad hoc networks. The DCA is distributed among the cluster heads (CHs) which become the shareholding DCA nodes. Thus, no single CH knows the DCA private key and when a new CH joins the backbone it needs to be issued with a share of the DCA's private key. In this scheme, when a node wants the DCA to sign a request, the node's CH receives the request and forwards it to the backbone. Any CH that receives the request uses his share of shared key to sign the request and produces a signature share. Once the node has received and verified k signature shares it can use them to construct the DCA's signature on request. This DCA supports the operations such as system setup or bootstrapping, applying a DCA private key, joining a new CH, evicting an existing CH, refreshing CH shares. In Bootstrapping operation, to construct the shared key and establish a (k,n) threshold sharing of a private key, all CHs must participate with the Distributed Key Generation algorithm as part of the construction of the NTDR backbone.

Rao and Xie [8] present another distributed certification authority scheme based on clustering scheme. They classify MANET nodes into clients, repositories, and server nodes. The client nodes are organized into clusters. In each cluster, some nodes are elected to be repository which stores the certificates of the nodes and servers within the cluster. The server nodes are elected in repository nodes. Because authentication is one of the key vulnerabilities of CA systems, they use a registration authority (RA). When a new node joins the network, it contacts a fixed RA. Then RA verifies credential of new node and contacts k server nodes. In addition, they issue certificate for new node and sent it to RA. Considering next step, RA gives this certificate to new node. Unfortunately, they have assumed that the RA does not

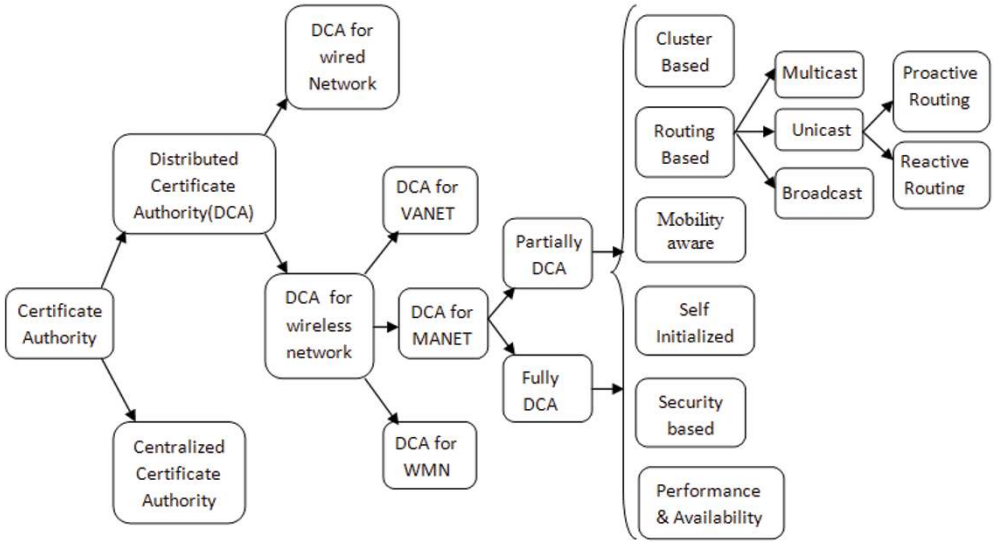

Figure 2 Taxonomy and classification of CA systems.

belong to ad hoc network and it is part of a wired network. To design various components of ad hoc network, we should preserve the independence of MANET and do not depend on any other networks' components. Certificate revocation lists (CRLs) are the other issues that have been discussed in this approach. Revoking a certificate can be initiated either by few nodes belonging to the same cluster or by a node that wants to revoke its own certificate. Furthermore, they have considered the mobility of nodes among clusters of MANET, something that almost never discussed in other schemes. When a mobile node leaves the source cluster and enters the destination cluster, it contacts any repository at destination cluster. At the same time, the mobile node sends its own certificate to the repository of destination cluster. The certificates of the node in the source cluster can be removed, unless the mobility management protocol predicts that the node is temporarily moved to a new cluster.

Elhdhili et al. [9] propose a totally distributed cluster-based key management for ad hoc networks and use a (K,N) threshold scheme to distribute an RSA signing key to the set of CHs, Furthermore, they use proactive and verifiable secret sharing to protect the secret from various attacks. They also assume that the system contains three types of nodes. The first one is an administrator that will exist only when the initialization step can leave the network. The second nodes are a set of CHs and the third ones are regular nodes. In addition, the administrator and CHs have directories to save the certificates. Each CH is a central CA for its cluster members. It is initialized by the administrator or by a coalition of K, other CHs. For system bootstrapping, administrator plays the role of a certification authority for CHs and then he can leave. Its main role is to certify existing CHs, distribute his secret key over them according to the secret sharing scheme and give them his certificate. The CHs will be considered as a distributed certification authority for the new nodes. In Figure 3, we have specified the advantages of clustering in DCA systems and the functions that CH can do on behalf of other users.

Dong et al. [6] have designed another cluster-based PDCA for MANET and propose optimization for DCA's nodes operations. First, when a user needs PDCA services, he must locate enough PDCA server nodes. To solve this problem, they shift the responsibility of CA discovery from user nodes to the CHs. Thus, a CH must maintain the required information to locate the CA nodes in or out of its cluster. Therefore, each CH maintains a CA information table (CIT), which contains a list of the CA nodes in its local cluster, and probably the CA information in other clusters. When a user requests DCA services, he sends it to his CH to obtain the required CA information through which the CA servers can quickly be located. In this way, DCA information is managed only among the CHs, which reduces the response time and overhead of various DCA operations and enhance the availability and response time of the system. Second, to increase the security of DCA, each node's share must be updated regularly, so the efficient updating of this secret shares in all CA server nodes is very important and has direct impact on DCA's performance. In this approach, they have devised a distributed scheme called sequential share update, to reduce the update overhead. It can resolve the multiple

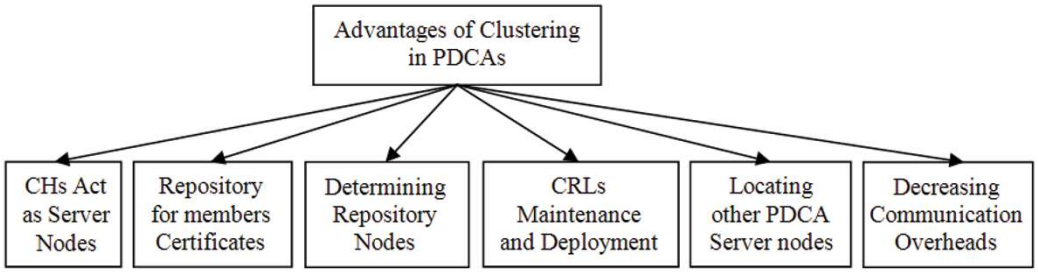

Figure 3 Advantages of clustering in DCA.

initializations problem and achieves fast system-wide update with low system overhead. At the beginning of sequential update, a coalition of t servers, instead of all servers, update their shares by applying the traditional proactive share update scheme. The remaining nodes will implement the self-initialization protocol so they can refresh their secret share with the help of t servers who have already updated their shares. Finally, although they have devised good solutions to increase availability and performance of DCA, they did not propose anything about RA in their scheme and just assume when a user first joins the network, he has been authenticated.

Lee and Jeong [10] proposed a partially distributed certificate management system that can handle mobility of nodes. It minimizes routing loads and enhances expandability of network by allowing participating nodes to authenticate each other without being interrupted by joining the cluster. In their model, certificate creation time slightly rose as the number of bits increased. But, the pace of increase was much slower than that obtained from the use of existing certificate-based authentication protocol. In addition, the proposed model offered a steady delivery time in the certificate creation phase despite the increase in packet size. The efficiency and security can be therefore maintained in the network. It was also found that the efficiency of the network was not influenced by changes in the number of nodes (k) because partial certificates are consistently generated by coalition of existing member nodes without being interfered by nodes joining the cluster. Since the node requesting partially distributed certificates performs the whole process involving certificate creation, unnecessary system overhead can be eliminated.

Zouridaki et al. [11] designed an elliptic curve-based DCA system. Elliptic curve is used because of its shorter key length and lower computational overhead. Their scheme uses a three-tiered logical view of DCA architecture. At the lowest tier, individual nodes are organized into clusters. The next tier consists of one or more certificate repositories in each cluster that broadcast the certificates of new nodes and the top tier consists of DCA servers that periodically inform the cluster about issued or the updated CRL. In general, the inter-cluster communication depends on whether it needs to be authenticated or encrypted, but the communication inside a cluster is relatively fast. Because each node caches the most used certificates and updated CRLs of the nodes within the cluster and infrequently communicates with the repositories. In this scheme, the number of servers is defined by $n = 2k + 1$ and it tolerates k compromised server in a predefined period of time. In Table 4, we have compared the various properties of all cluster-based DCA schemes.

4.2. Routing-based DCA

Even though flooding the messages in the network is the easiest way to transfer the certificate requests and other messages, it degrades the performance of MANET, so unicast protocols have been used in most of the DCA schemes to solve this problem. In MANETs, unicast routing protocols are classified into proactive, reactive, and hybrid protocols. With the large amount of control data that proactive routing protocols send, it seems that they can be used for implementing DCA in MANET. So, Dhillon et al. [5] propose an FDCA to be implemented with OLSR protocol. This approach uses existing OLSR control packets. It enables MANET to autonomously self-secure itself without any external administration and minimizes the signaling overhead. It is assumed that the network is initialized with at least k shareholders and a certificate-requesting node must discover them. Each MPR uses its TC message to announce which nodes in its MPR selector set claim to be shareholders. When a node receives TC messages, it uses them to build routing and shareholder tables. A node chooses a serving coalition of the k least costly shareholders in terms of hop count and sends a CREQ message to these nodes. Upon receiving this message, each node generates a certificate and returns it in a CREPLY message. The requesting node verifies the validity of the partial signature using verifiable secret sharing techniques. Upon receiving k valid replies, the

Table 4 Properties of cluster based DCA schemes

Ref #	Node type	Authentication	Certificate storage	Security	Other capabilities
[6]		Assume users have been authenticated		Sequential share update	CA node discovery by CHs
[2]	Cluster members & CHs			Evicting a CH, refreshing CH shares	Support for joining a new CH
[8]	Clients, repositories, server nodes	By fixed RA	Clusters repository nodes	Certificate revocation by CRLs	
[9]	Administrative nodes, CH nodes, regular nodes	Inter cluster authentication	Directories in administrators & CHs	Secure inter cluster communication	Self-initialization
[10]		Participating nodes authenticate each other			Nodes requesting certificate perform the whole process
[11]	Individual nodes, certificate repositories, DCA servers	Used in Inter-cluster communication	One or more certificate repositories	Elliptic curve, CRLs, secure communication between clusters	

requesting node adds them together and generates a proper signature. Unfortunately, the OLSR protocol does not support any security mechanism and attackers can alter control packets or send incorrect control packets. Also attacker may broadcast HELLO messages specifying neighbors that do not exist and becomes an MPR or he may send TC messages to be MPR and launch black hole attacks. To solve these problems, they use encryption and digital signatures to ensure the integrity and authenticity of the HELLO and TC messages.

Another OLSR-based scheme is proposed by Xia et al. [12]. They use identity-based encryption and alter the OLSR's HELLO and TC messages for sending the control data. However, there are two problems for implementing identity-based FDCA in MANET, the distributed generation of master keys and distribution of private keys. To solve these problems, they propose to distribute the master key share with threshold secret sharing and use of identity-based signcryption mechanism to provide a security channel for distributed private key generation.

In addition, because the identity-based encryption can reduce the communication overhead and resource consumption, the proposed approach is more suitable to the characteristics of the MANET.

Previous schemes were based on proactive routing, Yi and Kravets [7] present a PDCA scheme that uses reactive routing and call it MObile CA (MOCA). Any client who needs a certificate must contact at least k MOCAs. The contacted MOCAs generate a partial signature over the received data and client collects at least k partial signatures to construct the full signature. They also propose a protocol called MOCA certification protocol (MP), to provide an efficient way for communication between clients and MOCA nodes. If too few CREP packets are received, the client timeout and the certification request fail. So, setting the right value for this timer is very important. As a CREQ packet passes through a node, a reverse path to the sender is established. These reverse paths are coupled with timers and maintained long enough for a returning CREP packet to be able to travel back to the sender. The simplest method to reach MOCAs is the flooding of CREQ packets. To reduce the overhead of flooding, they introduce B-unicast, where the client can use multiple unicast to replace flooding of CREQs. It utilizes the existing information in the route cache and just uses flooding when there are not enough routes cached. If the network has low mobility, having just k cached routes may be sufficient. But, in highly mobile networks, sending exactly k unicast CREQs is dangerous since one CREQ loss results in the failure of certification request. Therefore, the node should send additional CREQs. Setting the right amount of these messages depends on the mobility of network. There are schemes that are based on MOCA and try to extend its functionality. For example, Sen et al. [13] designed a MOCA-based scheme and developed a reliable protocol with less communication overhead compared to the original MOCA. Their protocol uses the CREQ and CREP messages that can be piggybacked on the routing packets for reducing the communication overhead. The revocation of certificates is another issue that has been considered in this scheme. It is only possible when at least k CA nodes put their partial signatures on it. Each of the k CA nodes broadcasts the certificate to be revoked after putting its own signature. When the certificate to be revoked gathers k - 1 such partial signatures and reaches another CA node, it completes the signature, revokes the certificate, and broadcasts the revoked certificate to other CA nodes for updating their local CRLs. Network partitioning is one of the major problems that DCA scheme has to deal with it, in this scheme, it is handled by the transitive

Table 5 Properties of routing based DCA schemes

Ref #	Routing Protocols	Optimization	Security	Other capabilities
[5]	OLSR	Use TC and Hello messages	Encryption and digital signatures to protect TC & Hello messages	Choosing DCA server nodes based on hop counts
[12]	OLSR	Use TC and Hello messages	Identity-based encryption	Reduce communication overhead
[7]	Reactive routing protocols	MP or MOCA Certification protocol, B-unicast to replace flooding	Utilize route cache information, creating reverse path in CREQ forwarding	
[13]	Reactive routing protocols	Piggybacking of CREQ & CREP on the routing packets	CRLs maintenance and deployment	Handle network partitioning

delegation of CA responsibilities. Thus, an ordinary node that has recently authenticated itself by communicating with k CA nodes will be temporarily deputed to act as a CA node until the partition problem gets over.

In Table 5, we have specified the important properties of routing-based DCA schemes so it gives us appropriate details about these schemes.

4.3. Self-initialized schemes

In MANETs, it is very important that DCA schemes be self-initialized and the system authority exists only at the beginning of the network startup. So, a number of schemes have been proposed that support this property, for example, Ge and Lam [14] present a self-initialized DCA or SDCA that combine the advantages of the DCA and certificate chain schemes. They claim that this scheme addresses the scalability of certificate chain and has low cost, high availability, and security. In this scheme, the participating nodes initialize CA with the self-initializing protocol (SIP). With this protocol, the fundamental parameters of the DCA, such as the total number of DCA members, threshold value, and list of DCA members, will be negotiated and agreed among a certain number of nodes. With these parameters, the DCA is then constructed collaboratively by the involving nodes and without a trusted dealer. Another scheme for self-initialized DCA in ad hoc network is introduced by Kang et al. [15]. Their scheme uses proxy and threshold signatures. In this scheme, chair nodes that can distribute partial proxy keys for proxy nodes are authenticated by the system authority. In addition, proxy nodes that can issue certificates for other nodes are authenticated and initialized by the system authority or the chair nodes.

4.4. Mobility aware schemes

The mobility of DCA nodes in MANET has direct impact on DCA operations. If we do not find k DCA node, the certificate cannot be created. In Figure 4, we have classified different kinds of mobility that DCA nodes can show.

Pereira et al. [16] propose a self-adaptable and intrusion tolerant CA, that is able to manage changes in the membership of the servers group and allows the CA to reconfigure itself for guaranteeing the availability and the inviolability of the certification service.

Another solution is to increase the number of shares per node. Joshi et al. [4] have used this approach and proposed a secure, redundant, and fully distributed key management scheme for MANET. As a result, the number of nodes required to recreate the CA key is reduced and the probability of creating the certificate for normal users increases. System decreases and an attacker may compromises the CA key. Therefore, to increase security, intrusion detection systems must be used for identifying and removing the misbehaving or compromising nodes and the q shares chosen at random.

Luo et al. [17] proposed a solution called DIstributed CerTification Authority with probabilisTic freshness (DICTATE). They tried to enhance the security of an ad hoc network under the responsibility of a mother certification authority (mCA). Since the nodes can frequently be isolated from the mCA there is still a need to access to a certification authority. The mCA preassigns a special role to several nodes called servers that constitute a distributed certification authority during the isolated period. This solution ensures that the DCA always processes a certificate update or query request in a finite amount of time and that an adversary cannot forge a certificate. Moreover, it guarantees that the DCA responds to a query request with the most recent version of the queried certificate in a certain probability;

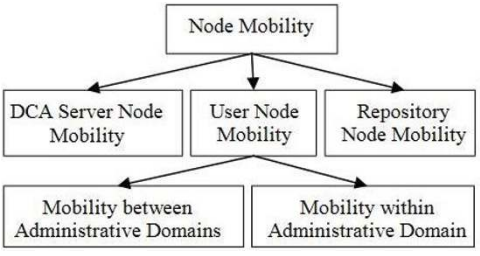

Figure 4 Different kinds of node mobility in DCA systems.

this probability can be made arbitrarily close to one, but at the expense of higher overhead.

4.5. Security-based schemes

Some of the presented schemes for DCA try to improve DCA's security and guard it against various attacks. For example, Zhou et al. [18] have designed a scheme called multiple-key cryptography-based DCA (MC-DCA) which is resilient to Sybil attacks. It achieves lower communication overhead and moderate latency compared with the threshold-based schemes. The Sybil attack is fatal to the threshold scheme. There is no efficient way to defeat it. In MANET, attackers can forge the IP and hardware addresses easily, so a malicious node impersonates many identities and it is difficult to bind a single identity with one node.

Also, Rajaram and Palaniswami [19] designed a high performance CA that supports certificate renewal, revocation, and resists to various outside attacks. Their scheme supports routing cum forwarding (RCF) of packet monitoring, certification revival, and certificate revocation. By monitoring RCF behavior, the malicious nodes are detected by monitoring the behavior hop-by-hop. Certificate revival uses a redundancy scheme in which a node is allocated more than one key share by incorporating redundancy into the network. This mechanism guarantees that genuine nodes can continue to stay in the network by revival of their certificates along a periodical time period. Certificate revocation provides the authority to isolate any malicious nodes or regain the nodes which turn up to its best state after any attack or failure.

In Figure 5, we have specified the security techniques that can be applied in DCA systems. It is obvious that none of these methods can provide security and we must apply all of them to provide a secure DCA scheme.

4.5. Performance- and availability-based schemes

In general, when we distribute the task of one system to many subsystems, we may have availability and performance problems. So, some of the DCA schemes try to decrease these problems and use special infrastructures to provide better availability and performance. For example, Raghani et al. [20] have designed a DCA, in which networks nodes can obtain certificate from their one hop neighbors. With such distributed CA, when the number of neighbors of a node, also called node degree, reduces, there is a substantial increase in the certification service delays. Therefore, they have tried to solve this problem with a suite of network monitoring protocols. The proposed protocols dynamically adjust the threshold value by monitoring the average node degree of the network and thereby prevent an increase in certification service delay.

We have compared the properties of various proposed DCA schemes at Table 3. This comparison gives us good insight on the proposed schemes and determines the less researched areas that can be studied in future works.

5. Design goals

Chaddoud et al. [2] have proposed some properties for DCA systems in MANETs. We complete these properties by adding important issues, which are required for MANET environments:

- **Availability**

  Like the normal user nodes, the DCA shareholding nodes may move to the other places and be inaccessible to the user nodes. In this condition, a user node may not find the required k DCA server node. Thus, a DCA scheme must take into account the mobility of DCA server nodes and dynamic nature of a MANET and propose appropriate solutions to solve these problems. For example, in some schemes, this problem is solved by allocating more than one share to each DCA server node.

- **Security**

  To avoid the single point of failure, no important system secret must be allocated to a single node and DCA key pairs must be generated in a distributed way. Also, a key refresh protocol is required to ensure that the lifetimes of critical keys are restricted. In addition, intra DCA data must be secured with encryption or digital signatures.

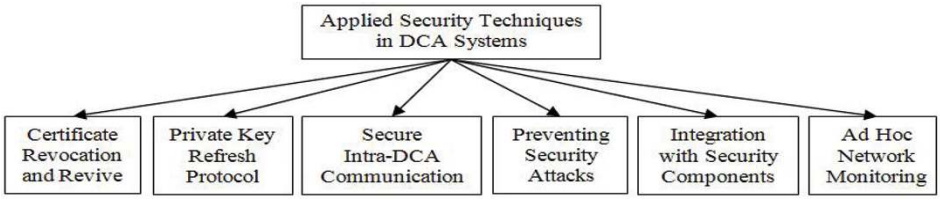

Figure 5 Techniques for providing security in DCA systems.

- **Reliability**

DCA system should avoid relying solely on the underlying communication network, since channels or nodes may be compromised. Where possible, measures should be taken to improve system robustness. Use of encryption and digital signature for inter DCA node communication can improve DCA's security.

- **Efficiency**

MANET nodes are power and bandwidth limited and communication is relatively slow and unreliable, so protocols should attempt to minimize the amount of transmitted data between nodes.

- **Fault tolerance**

The main concern of fault tolerance is the capability to maintain correct operation in the presence of faulty nodes. If a node is malfunctioning and other nodes can observe such malfunctions, a certain level of recovery is possible. For example, some schemes such as MOCA employ intelligent replication using threshold cryptography to provide tolerance of faulty nodes.

- **User node mobility**

DCA system must support two kinds of mobility in MANET, first client nodes mobility, and second DCA server nodes mobility. In first case, client nodes may change their position or travel other clusters, so it is desirable that user can use the DCA system even in the destination cluster or position. Also, we can consider two kind of client nodes mobility, nodes mobility inside the nodes administrative domain and between the administrative domains.

- **Self-initialization**

It is better that schemes work in a self-initialized manner where the system authority exists only at the beginning of the network operation, or system work by itself without any administrative interventions.

- **Conformance to network properties**

A DCA system is a layer above the ad hoc network. It uses MANET services to process user requests. Thus, it will be more cost-effective that DCA system uses the existing protocols and infrastructures efficiently. For example, if the clustering has been used in MANET, it is better to use it, or if MANET uses some proactive routing protocol, it is better to use its control packets for piggybacking required data.

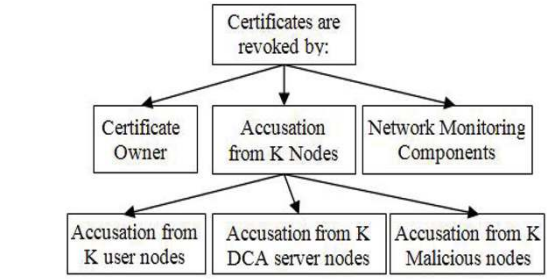

Figure 6 The reasons of certificate revocation.

- **Conformance to network size**

The type of DCA system used depends on the MANET size. So, with few numbers of nodes we can use FDCA schemes and with the large number of nodes, PDCA schemes can be used.

- **Integration**

A DCA system is not a standalone system. It must cooperate with the other security components and should be easily integrated with the other systems such as registration authorities or user applications. This can be achieved by using standard algorithms and methods in all security programs. For example, certificate and CRLs must be according to the X.509 standards.

- **Scalability**

It is normal that the performance of the DCA system decrease with the expansion and growth of

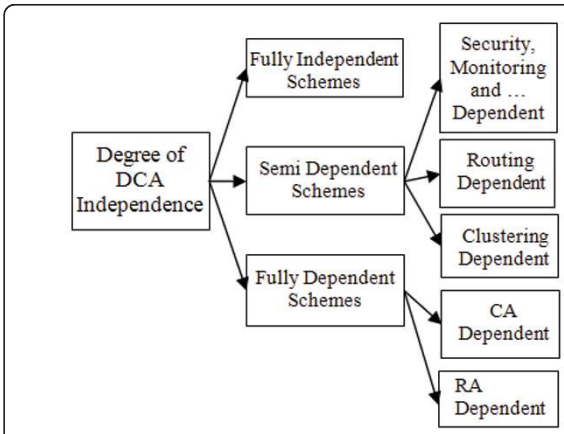

Figure 7 Different levels of Independence in DCA schemes.

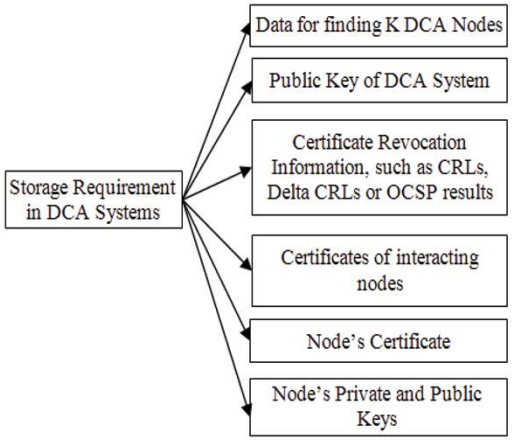

Figure 8 Required storages for implementing PKI.

network. So, the collection of shareholding nodes must be proportional to the number of normal nodes over the time. Thus, we require protocols to enable shareholding DCA nodes to leave and join the DCA system.

- **Certificate revocation and validation**

It is better that DCA not only supports operations such as issuing and management of certificates, but also supports revocation and validation of issued certificates. These operations are done using CRLs or OCSP protocol. Figure 6 shows the components and reasons that indicate why the certificates can be revoked. As one can see from this figure, unlike Internet, MANET members can accuse other nodes and revoke the certificate of malicious nodes.

- **Independence**

A DCA system like the other distributed systems should not depend on central components. It must be designed and built without any reliance on any components of fixed or wired networks. Figure 7 shows different levels of independence in DCA schemes: fully independent, semi-dependent, and fully dependent DCA schemes.

Semi-dependent schemes depend on the other MANET components and services. But, fully dependent schemes depend on the wired networks components such as RAs or CAs.

- **Low storage overhead**

A PKI system requires large amount of storage for storing its certificate, keys, and other data structures. Although this property of PKI is not very important on Internet, it can create some problems in resource limited networks including MANETs. Therefore, an ideal DCA system must have low storage overhead and do not waste limited storages of mobile devices. In Figure

Table 6 Comparison of proposed DCA Schemes

DCA scheme no	FDCA or PDCA	Routing based	Cluster based	Self-initialized	DCAmobility support	User node mobility support	Security based	Performance	Certificate revocation support
2	PDCA	-	Yes	-	-	-	-	-	-
3	FDCA	Yes	-	-	-	-	Yes	-	-
4	PDCA	-	Yes	-	-	-	-	-	-
5	PDCA	-	Yes	-	-	Yes	-	-	Yes
6	PDCA	-	Yes	Yes	-	-	Yes	Yes	Yes
7	PDCA	-	Yes	-	-	-	-	-	-
8	PDCA	-	Yes	-	Yes	Yes	Yes	Yes	Yes
9	FDCA	Yes	-	-	-	-	Yes	-	-
10	PDCA	Yes	-	-	Yes	-	-	Yes	Yes
11	PDCA	Yes	-	-	Yes	-	-	Yes	Yes
12	PDCA	-	-	Yes	-	-	Yes	Yes	-
13	FDCA	-	-	Yes	-	-	-	-	Yes
14	PDCA	Yes	-	Yes	Yes	Yes	-	Yes	-
15	FDCA	-	-	-	Yes	Yes	Yes	-	Yes
16	PDCA	-	-	-	Yes	Yes	Yes	Yes	Yes
17	PDCA	-	Yes	-	-	-	YES	-	-
18	PDCA	-	-	-	-	-	Yes	Yes	Yes
19	PDCA	-	-	Yes	-	-	Yes	Yes	-

8, we have shown various information that a DCA scheme should store in a DCA client node.

Although, it is desirable that an ideal DCA has all these properties, some of them are in contradict to each other. For example, to support DCA nodes mobility, some schemes allocate more than one share to each DCA server node, so achieve mobility with the cost of decreased security. The properties of 18 DCA schemes proposed for MANETs have been compared in Table 6.

6. Conclusion and future works

Security of MANET is one of the challenging issues. Many schemes have been proposed to increase the security of this kind of networks. PKI has provided many security services in wired and fixed networks; so many schemes try to adapt PKI components such as CAs to special characteristics of MANETs. In this article, we classified various DCA schemes and investigated pros and cons of them. This classification can help us to better understand the applied techniques in DCA systems and propose more appropriate solutions or upgrade existing ones. Also, it shows us that the areas that are less investigated or properties that are less supported. For example, although the communication pattern in DCA is one-to-many but none of the studied solutions have used multicast routing, or with the greater need on security none of the schemes have used secure routing protocols. Thus, many aspects of DCA systems must be investigated and evaluated to achieve better performance, scalability, and security.

Author details
[1]Science and Research Branch, Computer Engineering Department, Islamic Azad University, Tehran, Iran [2]North Tehran Branch, Computer Engineering Department, Islamic Azad University, Tehran, Iran [3]Iran Telecommunication Research Center, ITRC, Tehran, Iran [4]Computer Engineering Department, Urmia University, Urmia, Iran

Competing interests
The authors declare that they have no competing interests.

Received: 23 February 2011 Accepted: 27 September 2011
Published: 27 September 2011

References

1. WE Anderson, JT Michalski, BP Van Leeuwen, Enhancements for distributed certificate authority approaches for mobile wireless ad hoc networks, Technical Report, Sandia National Laboratories, (2003)
2. G Chaddoud, K Martin, Distributed certificate authority in cluster-based ad hoc networks. Wireless Communications and Networking Conference. **2**, 682–688 (2006)
3. L Zhou, RV Renesse, FB Schneider, Coca: a secure distributed online certification authority. Journal ACM Transactions on Computer Systems (TOCS). **20**(4), 329–368 (November 2002). doi:10.1145/571637.571638
4. D Joshi, K Namuduri, R Pendse, Secure, redundant, and fully distributed key management scheme for mobile ad hoc networks: an analysis. Journal EURASIP Journal on Wireless Communications and Networking, 579–589 (2005)
5. D Dhillon, TS Randhawa, M Wang, L Lamont, Implementing a fully distributed certificate authority in an OLSR MANET, in *Wireless Communications and Networking Conference* **2**, 682–688 (2004)
6. Y Dong, AF Sui, SM Yiu, VOK Li, LCK Hui, Providing distributed certificate authority service in cluster-based mobile ad hoc networks. Computer Communications **30**, 2442–2452 (2007). doi:10.1016/j.comcom.2007.04.011
7. S Yi, R Kravets, MOCA: mobile certificate authority for wireless ad hoc networks. The Second Annual PKI Research Workshop (PKI) (2003)
8. W Rao, SH Xie, Merging clustering scheme in distributed certificate authority for ad hoc network, in *IET International Conference on Wireless, Mobile and Multimedia Networks*, 1–4 (2006)
9. ME Elhdhili, LB Azzouz, F Kamoun, A totally distributed cluster based key management model for ad hoc networks. the Third Annual Mediterranean Ad Hoc Networking Workshop (2004)
10. DY Lee, HC Jeong, An efficient certificate management for mobile ad-hoc network, in *5th International Conference on Mobile and Wireless Networks*, 355–364 (2006)
11. C Zouridaki, BL Mark, K Gaj, RK Thomas, Distributed CA-based PKI for mobile ad hoc networks using elliptic curve cryptography. First European PKI Workshop: Research and Applications EuroPKI 232–245 (2004)
12. P Xia, M Wu, K Wang, X Chen, Identity-based fully distributed certificate authority in an OLSR MANET, in *4th International Conference on Wireless Communications, Networking and Mobile Computing*, 1–4 (2008)
13. J Sen, MG Chandra, P Balamuralidhar, SG Harihara, H Reddy, A scheme of certificate authority for ad hoc networks, in *18th International Workshop on Database and Expert Systems Applications*, 615–619 (2007)
14. M Ge, K Lam, Self-initialized distributed certificate authority for mobile ad hoc network, in *3rd International Conference and Workshops on Advances in Information Security and Assurance*, 392–401 (2009)
15. J Kang, D Nyang, A Mohaisen, YG Choi, Certificate issuing using proxy and threshold signatures in self-initialized ad hoc network, in *international conference on Computational science and its applications*, 886–899 (2007)
16. FC Pereira, JD Silva fraga, RF Cust'odio, Self-adaptable and intrusion tolerant certificate authority for mobile ad hoc networks, in *22nd International Conference on Advanced Information Networking and Applications*, 705–712 (2008)
17. J Luo, JP Hubaux, PT Eugster, Dictate: distributed certification authority with probabilistic freshness for ad hoc networks. IEEE Transactions on Dependable and Secure Computing 311–323 (2005)
18. H Zhou, MW Mutka, LM Ni, Multiple-key cryptography-based distributed certificate authority in mobile ad-hoc networks, in *Global Telecommunications Conference*, 5 (2005)
19. A Rajaram, S Palaniswami, High performance certificate authority scheme in MANET. International Journal of Computer and Network Security 106 (2010)
20. S Raghani, D Toshniwal, R Joshi, Dynamic support for distributed certification authority in mobile ad hoc networks, in *International Conference on Hybrid Information Technology*, 424–432 (2006)

doi:10.1186/1687-1499-2011-112
Cite this article as: Masdari *et al.*: **A survey and taxonomy of distributed certificate authorities in mobile ad hoc networks.** *EURASIP Journal on Wireless Communications and Networking* 2011 **2011**:112.