IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

SPECIAL SECTION ON ROADMAP TO 5G: RISING TO THE CHALLENGE

Received March 22, 2019, accepted April 25, 2019, date of publication May 1, 2019, date of current version May 17, 2019.

Digital Object Identifier 10.1109/ACCESS.2019.2914359

Key Management for Beyond 5G Mobile Small Cells: A Survey

MARCUS DE REE[1,2], GEORGIOS MANTAS[1,3], (Member, IEEE), AYMAN RADWAN[1], (Senior Member, IEEE), SHAHID MUMTAZ[1], (Member, IEEE), JONATHAN RODRIGUEZ[1,2], (Senior Member, IEEE), AND IFIOK E. OTUNG[2]

[1]Instituto de Telecomunicações, 3810-193 Aveiro, Portugal
[2]Faculty of Computing, Engineering and Science, University of South Wales, Pontypridd CF37 1DL, U.K.
[3]Faculty of Engineering and Science, University of Greenwich, London SE10 9LS, U.K.

Corresponding author: Marcus de Ree (mderee@av.it.pt)

This research work leading to this publication received funding from the European Union's Horizon 2020 Research and Innovation programme under grant agreement H2020-MSCA-ITN-2016-SECRET-722424. The authors would also like to acknowledge the collaboration with the EU-INDIA ICI+/2014/342-896 REACH project.

ABSTRACT The highly anticipated 5G network is projected to be introduced in 2020. 5G stakeholders are unanimous that densification of mobile networks is the way forward. The densification will be realized by means of small cell technology, and it is capable of providing coverage with a high data capacity. The EU-funded H2020-MSCA project "SECRET" introduced covering the urban landscape with mobile small cells, since these take advantages of the dynamic network topology and optimizes network services in a cost-effective fashion. By taking advantage of the device-to-device communications technology, large amounts of data can be transmitted over multiple hops and, therefore, offload the general network. However, this introduction of mobile small cells presents various security and privacy challenges. Cryptographic security solutions are capable of solving these as long as they are supported by a key management scheme. It is assumed that the network infrastructure and mobile devices from network users are unable to act as a centralized trust anchor since these are vulnerable targets to malicious attacks. Security must, therefore, be guaranteed by means of a key management scheme that decentralizes trust. Therefore, this paper surveys the state-of-the-art key management schemes proposed for similar network architectures (e.g., mobile ad hoc networks and ad hoc device-to-device networks) that decentralize trust. Furthermore, these key management schemes are evaluated for adaptability in a network of mobile small cells.

INDEX TERMS 5G, beyond 5G, decentralized systems, device-to-device communication, key management, mobile small cells, security, small cells, wireless ad hoc networks.

I. INTRODUCTION

It has been almost a decade since the 4G mobile network was introduced. Since that time, many more users and wireless devices have joined the network. The number of wireless devices connected to the network is expected to have grown by a factor somewhere between 100 and 10,000 by 2021 [1]. These devices range from PDAs to smartphones, tablets and machines falling within the Internet of Things (IoT) concept [2], [3]. Furthermore, demanded mobile data is expected to have increased by a factor of 1,000 per device by 2021 [1], [4]. This surge puts a lot of pressure on the current 4G network. This causes a reduction in data rates and it increases latency and signal interference.

To address these challenges, new technologies are emerging to create the next generation 5G network [5]–[9]. These technologies will deliver higher network capacity, allow the support of more users, lower the cost per bit, enhance energy efficiency and provide the adaptability to introduce future services and devices. It is envisioned that the 5G network will be deployed by 2020 and beyond [1], [5], [6], [10] with data rates reaching speeds up to 10 Gb/s and delays as low as 1 ms end-to-end.

One of these emerging technologies is small cells. The small cell technology is the most effective solution to deliver ubiquitous 5G services in an energy efficient manner to its users. In particular, mobile small cells are proposed to cover the urban landscape. These can be set up on-the-fly, based on demand, using mobile devices (i.e. user equipment) or Remote Radio Units (RRUs) [11]. Mobile

The associate editor coordinating the review of this manuscript and approving it for publication was Muhammad Imran.

small cells are networks consisting of mobile devices which are within relative close proximity. This allows device-to-device (D2D) communications and enables high data rate services such as video sharing, gaming and proximity-aware social networking. Mobile small cells therefore negate the necessity for network operators to install and maintain additional network infrastructure. End-users are provided with this plethora of 5G broadband services while D2D communications improve throughput, energy efficiency, latency and fairness [12]–[14].

The current network infrastructure guarantees secure data transmissions between network subscribers with the distribution of cryptographic keys present in SIM cards. These keys are used to authenticate network subscribers, provides access to network resources and establishes a secure channel between the mobile device and the network infrastructure. In order to set up secure D2D communications, mobile devices require cryptographic keys which are shared between each other. These keys require updating mechanisms to guarantee privacy over an extended period of time and revocation mechanisms in the event that a mobile device is maliciously compromised and no longer correctly identifies the owner of the device. Providing secure communication in a network of mobile small cells requires its own key management scheme. Traditionally, a key management scheme relies on a centralized trusted third party (TTP). This TTP is considered to be trustworthy and secure by every user inside the network. It can therefore distribute cryptographic keys between any set of network devices to set up a secure communications channel.

A. CONTRIBUTION

This article surveys a wide spectrum of key management schemes proposed for securing mobile ad hoc networks (MANETs) as well as ad hoc D2D networks. A network of mobile small cells could be interpreted as a hybrid between these two types of networks, sharing many common network characteristics such as network nodes communicating in a multi-hop wireless fashion; network nodes function as both hosts and routers; these networks have a dynamic network topology; and these networks can be homogeneous or heterogeneous.

Key management schemes proposed for MANETs are self-organized during network deployment due to its inability to rely on an available and online centralized TTP. Numerous quality surveys exist which explore proposed key management solutions for MANETs [15]–[20]. These surveys describe individual key management schemes and evaluates them for general infrastructureless MANETs. However, mobile small cells are network infrastructure-assisted which provide opportunities when it comes to aspects such as key management and efficient routing.

Key management schemes proposed for ad hoc D2D networks consider the assistance of available network infrastructure, but do not take densification of the network into account. There are few quality surveys related to security for D2D communications. To emphasize, the quality surveys [21], [22] cover many aspects of D2D communications technology, however security was still mentioned as an open research problem. Recently, two surveys [23], [24] about security for D2D communications were published. These surveys cover key management proposals of which many either assume that the network infrastructure is secure against compromise or they do not consider multi-hop communication.

On the other hand, the key management schemes in our survey are selected based on their ability to self-organize the key management to secure multi-hop D2D communications without having to rely on a fixed intrastructure and an online centralized TTP. Furthermore, a key management classification is provided that categorizes various approaches of solving the key management. These approaches are treated as a collective of key management schemes and include work extending upon the original key management scheme. This provides a detailed and wide scope of the potential of a key management approach such that they can be properly evaluated for their adoptability to secure a network of mobile small cells. It has been the aim to include proposed mechanisms such as the network initialization, key generation, key distribution, key authentication, key update and key revocation. Details regarding the involved mathematics, algorithms or protocols are not discussed since these would not affect the outcome of the evaluation of the key management approach for adoptability in a network of mobile small cells covering the urban landscape.

B. STRUCTURE OF THE SURVEY

Section II provides a description of the envisioned network architecture in which mobile small cells enable the mobile devices equipped with D2D communications technology to communicate in a multi-hop wireless fashion. Each network characteristic is individually evaluated from a security and privacy standpoint and its challenges are described. Section III gives an overview of the evaluated self-organized key management approaches and provides a compilation of requirements which a self-organized key management scheme must satisfy in order to be suitable for adoption in a network of mobile small cells. The following sections describe and evaluate self-organizing key management schemes. Key management schemes in section IV rely on certificate-based public key cryptography (PKC), in section V they rely on identity-based PKC, in section VI they rely on certificateless PKC and in section VII they rely on symmetric key cryptography (SKC). Section VIII compares the evaluated key management approaches and highlights the main considerations affecting its adoptability. Section IX provides researchers with insight about designing a self-organized key management scheme for networks utilizing the network coding [25] paradigm. Finally, section X presents some uncovered open research problems and section XI draws conclusions and outlines future research

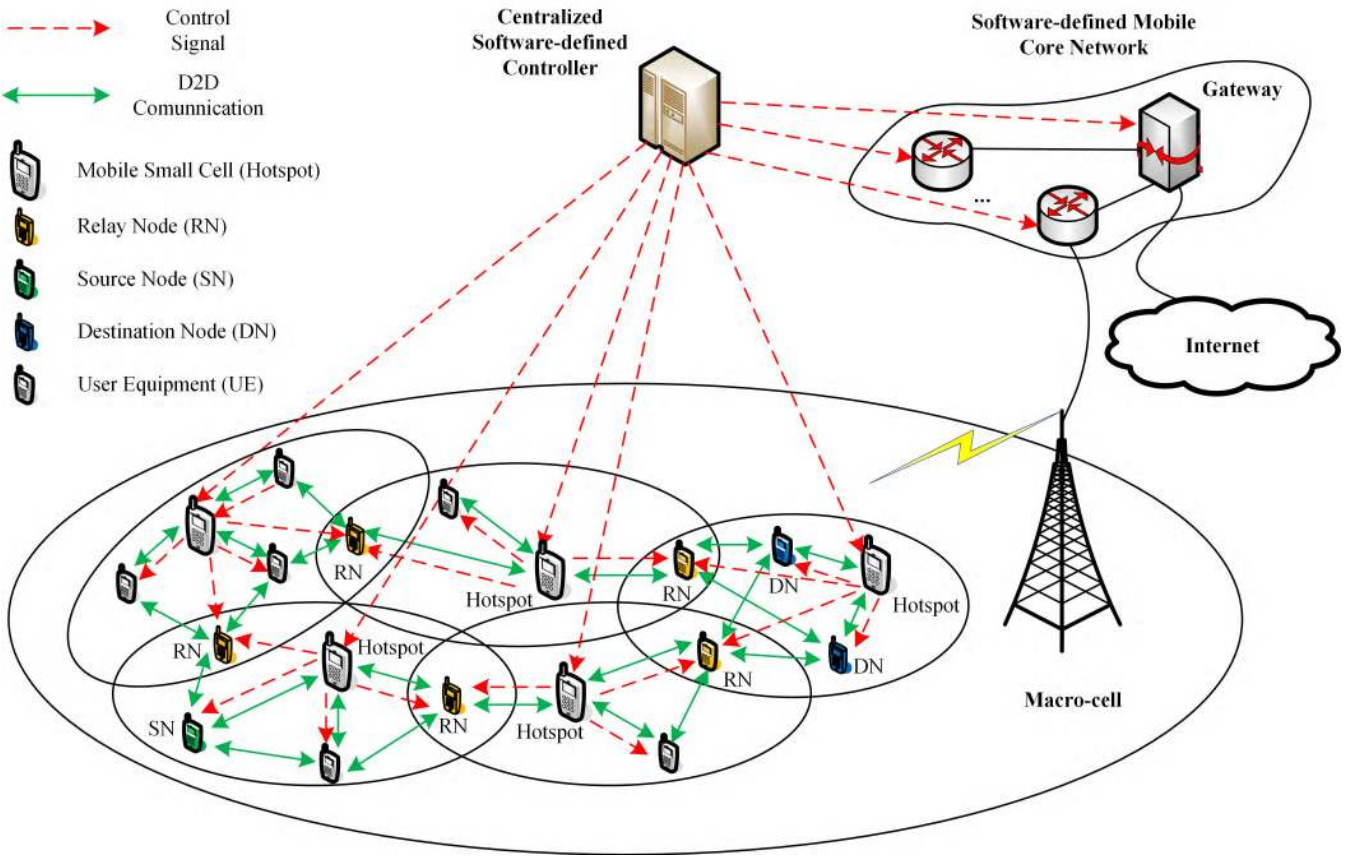

FIGURE 1. The scenario architecture as introduced by project "SECRET" [26].

directions to design novel key management schemes suitable for providing security and privacy in a network of mobile small cells.

II. MOBILE SMALL CELLS

A. A NETWORK OF MOBILE SMALL CELLS

The densification of the urban landscape by means of mobile small cells and network offloading by means of enabling D2D communications lead to a network which is capable of increasing data rates and energy efficiency while reducing latency and interference. However, many of these advantages can be credited to the introduction of ordinary small cells. Since the strength of a radio signal diminishes with the square of the distance, replacing large transmissions to and from the base station (BS) by multiple shorter transmissions provides significant energy savings. Similarly, the shorter and less powerful signals will reduce interference which allows for a higher throughput and thus increased data rates. Lower latency is realized by providing a more direct route between a source node (SN) and a destination node (DN). Nevertheless, mobile small cells provide additional advantages. They can be setup on-the-fly, based on demand, at any place, at any time, using existing mobile devices or Remote Radio Units (RRUs) [11]. This wireless ad hoc network can therefore function at a low cost since network operators are not required to install and maintain additional network infrastructure. Furthermore, mobile small cells support time and space varying traffic [27], [28].

The EU-funded H2020-MSCA project "SECRET" [29] introduces a scenario architecture for the next generation mobile network which provides opportunities for both network operators and network users. This scenario architecture is illustrated in Fig. 1.

The cellular network, consisting of macro cells is partitioned into a network (or cloud) of mobile small cells. Each of these is controlled and maintained by a hotspot (i.e. cluster-head). This is a mobile node within the cluster that is selected to become the local radio manager to control and maintain the cluster. In addition, each hotspot is controlled by a centralized software-defined controller. Through cooperation these hotspots form a wireless network that has several gateways/entry points to the mobile network using intelligent high-speed connections. Data traffic between mobile nodes is established through D2D communication.

Suppose that a mobile node wishes to share data with two other mobile nodes. The mobile node in possession of this data, the source node (SN), sends the data to the mobile nodes requesting the data, the destination nodes (DNs). Note that these mobile nodes are not required to be in the same mobile small cell as illustrated in Fig. 1. Using D2D communications

and multiple hops, the data is being routed through the network of mobile small cells from the SN to the DNs.

B. SECURITY AND PRIVACY CHALLENGES

The scenario architecture brings multiple networking technologies together. Each of these comes with security and privacy challenges. The privacy threats can be divided into two categories, identity privacy and data privacy. Identity privacy threats cover attacks in which the attacker uncovers identifying information about the sender or receiver, whereas data privacy threats cover attacks in which the attacker uncovers information about the transmitted data. The following sections identify the security and privacy challenges for each networking technology present in the scenario architecture.

1) MULTI-HOP WIRELESS COMMUNICATIONS

Allowing data to traverse multiple hops to reach its destination brings a spectrum of privacy threats. To establish secure communication between two mobile nodes, both nodes are required to prove their identity to each other while remaining anonymous to intermediate nodes. This challenge can be solved with anonymous mutual authentication. With anonymous mutual authentication, both mobile nodes participate in a so-called zero-knowledge proof of identity protocol. This protocol involves the exchange of challenges in which both nodes eventually prove their knowledge of a pre-established secret. This secret (or key) would only be known by these two nodes, therefore effectively identifying each other. Without initial identification, communication is susceptible to identity impersonation attacks. Furthermore, an intermediate node could modify or eavesdrop on data in transmission. These attacks are well studied and various cryptographic techniques are developed to counter these attacks. Data modification attacks can be detected using signature schemes and integrity schemes whereas eavesdropping can be prevented using data encryption schemes. However, each countermeasure requires the communicating nodes to be in possession of a pre-shared secret key [30], [31].

Multi-hop wireless communication is also affected by free-riding. Free-riding means that a mobile node acts selfishly, unwilling to route data to others while still requesting demanded data, for the purpose of increasing battery life. This reduces fairness and transmission availability within the network. Stimulating cooperation mechanisms are necessary to prevent free-riding and several solutions have been proposed [32]–[34].

2) D2D COMMUNICATIONS

The introduction of D2D communications technology poses location-based privacy challenges, since these data transmissions require relative close proximity between mobile nodes. This allows colluding users to perform a boundary attack to locate nearby mobile nodes. Zickuhr [35] conducted a survey and found that 46% of teen users and 35% of adults turn off location tracking features due to privacy concerns. These privacy concerns need to be addressed so that users will allow their devices to be discoverable and participate in routing data through D2D communications. Fortunately, location privacy can be guaranteed using the identity preserving techniques of anonymous mutual authentication [31]. As discussed previously, anonymous mutual authentication relies on pre-shared secret keys.

3) MOBILE SMALL CELLS

The introduction of mobile small cells defines the parties involved in the network. These involved parties are the mobile devices and the network infrastructure. Neither of these parties are considered capable of resisting compromise by a malicious attacker and therefore cannot act as the online centralized TTP. The online centralized TTP would be the single-point-of-attack within the network such that denial-of-service (DoS) attacks disable key management services. Therefore, the core issue of mobile small cells lies in the lack of a secure and trusted entity to establish security during network deployment. This lack of a trusted entity poses issues when it comes to the key management.

Key management schemes dictate how cryptographic keys are generated, distributed to network nodes, authenticated, updated, revoked and so on. These keys are then used to perform cryptographic schemes, like the ones discussed previously. Key management is therefore the building block upon which all security is based.

In the literature there has been key management schemes proposed for similar network architectures such as MANETs and ad hoc D2D networks, however these schemes are either incomplete (e.g., lacking key update or key revocation procedures), they rely on a secure routing protocol or they require some other form of a secure channel for (partial) key distribution which is difficult to realize in our scenario architecture. This exploration of security and privacy challenges demonstrates that cryptographic techniques and anonymous mutual authentication are able to provide secrecy and anonymity assuming that an underlying key management scheme can effectively support these. Therefore, it is of the utmost importance to design novel key management schemes which fit our scenario architecture. These schemes should provide robust and low complexity key management including secret key sharing among mobile nodes, key revocation, key update and mobile node authentication.

III. SELF-ORGANIZED KEY MANAGEMENT

A. OVERVIEW OF SELF-ORGANIZED KEY MANAGEMENT APPROACHES

Key management schemes can be classified in a variety of ways. In this article, we have classified each key management scheme by the form of cryptography which is used and therefore defines the method of key establishment and key authentication, the initial phases of key management. The authors consider key management schemes to be self-organizing when mobile devices do not have to rely on an online centralized TTP to provide key management

TABLE 1. Summarizing table of security and privacy challenges in the proposed scenario architecture.

Networking technology	Privacy threats	Countermeasures
Multi-hop wireless communications	Identity impersonation	Identification schemes
		Anonymous mutual authentication
	Data modification	Signature schemes
		Integrity schemes
	Eavesdropping	Data encryption schemes
	Free-riding	Cooperation mechanisms
D2D communications	Boundary attack	Anonymous mutual authentication
Mobile small cells	Lack of a trusted third party	Self-organized key management

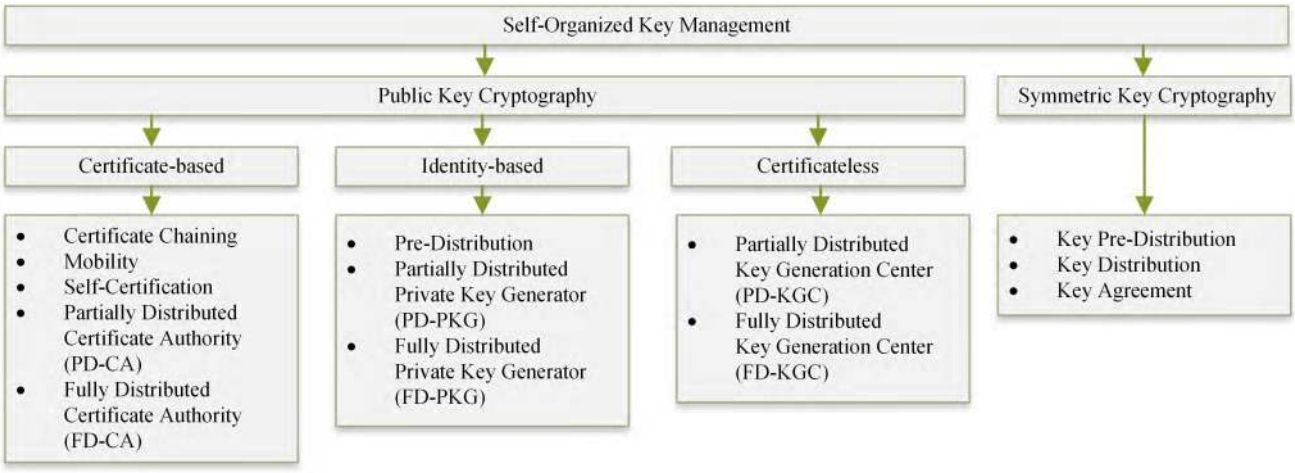

FIGURE 2. Classification of self-organized key management approaches.

services during network deployment. This classification of the proposed self-organized key management schemes discussed in this article are illustrated in Fig. 2.

In certificate-based public key cryptography (CB-PKC) [36], [37] every network node self-generates its own mathematically linked public and private key pair. Next, each node would contact the centralized TTP – also known as the Certification Authority (CA) – which verifies the identity of the network node and provides this node with a signed certificate containing the public key and the identity of its owner (among other information). This signed certificate could then be distributed throughout the network to nodes requesting to securely communicate with the owner of the certificate. The signature on the certificate can be verified such that the requesting node is confident that the public key on the certificate is authentic. Since a network of mobile small cells is unable to support an online centralized TTP, this article presents five approaches based on CB-PKC which propose alternative methods of providing a means to verify the authenticity of public keys.

In identity-based public key cryptography (ID-PKC) [38]–[40] the identity of a network node (e.g., network address, phone number) is used as a public key. This identity is public knowledge and does not require certificates to distribute this keying information through the network. However, corresponding private keys cannot be simply generated from a public key. Instead, private keys are provided by the centralized TTP – also known as the Private Key Generator (PKG) – after it verified the identity of the network node. Due to the inability to support an online centralized TTP in a network of mobile small cells, this article presents three approaches based on ID-PKC which proposes alternative methods to providing network nodes with authentic identity-based private keys.

In certificateless public key cryptography (CL-PKC) [41], [42] every network node combines two key pairs to establish secure communication. A network node creates a mathematically linked key pair, similar to the key pair used in CB-PKC, while also using its identity as a public key and its corresponding private key obtained from the centralized TTP – also known as the Key Generation Center (KGC) – after it verified the identity of the network node. Both of these key pairs would be used for securing communication. A network node wishing to communicate with the key pair owner would request the (certificateless) public

key and use this along with the owner's identity to secure communication. The (certificateless) public key does not require to be authenticated, since an adversary is unable to benefit from replacing the public key for a false one. This is due to the identity-based private key which is still unknown to the adversary. The provided public key and identity can therefore be used to secure communication, since only the owner of both possesses the corresponding private keys. Again, due to the inability to support an online centralized TTP in a network of mobile small cells, this article presents two approaches based on CL-PKC which proposes alternative methods to providing network nodes with authentic identity-based private keys.

Symmetric key cryptography encompasses three methods of establishing keys which can be verified for authenticity [36], [37]. These three methods are named key pre-distribution, key distribution and key agreement. For the key pre-distribution and key distribution method, a TTP – also known as the Key Distribution Center (KDC) – provides network nodes with keys. With key pre-distribution, every node receives a set of keys prior to network deployment such that each key is shared with one other node inside the network. The use of a particular key therefore informs both parties who they are communicating with, thus authentication is provided along with the keys from the KDC. Key distribution works similarly, however the keys are distributed on-demand and during network deployment. Key agreement is the only scheme which does not rely on a TTP. Network nodes wishing to set up a secure channel follow a protocol in which each node contributes some secret information to create a shared key. However, authentication is necessary to prevent a man-in-the-middle (MITM) attack, meaning that each network node must have a means to identify the other prior to establishing a shared key. This is only possible if each network node is in possession of some secret information that only they know, therefore relying on a pre-distributed secret or a public key management scheme. This article discusses research efforts following the symmetric key management approach, however no proposal was eventually found to be able to securely self-organize the key management in a dynamic network.

B. REQUIREMENTS OF SELF-ORGANIZED KEY MANAGEMENT FOR A NETWORK OF MOBILE SMALL CELLS

Many cryptographic security solutions are available to solve the security and privacy challenges in a network which combines multi-hop, wireless and D2D communications with mobile small cells. However, the difficulty of securing this network architecture comes from its reliance on a decentralized and efficient key management scheme to support these cryptographic security solutions. This subsection describes the seven requirements that a key management scheme must satisfy in order to be suitable as a valid candidate for adoption in a network of mobile small cells.

1) SECURITY

The most important requirement and the main principle on which cryptography is based on, providing security. The key management scheme is expected to provide key management services such that every network node is capable of establishing or obtaining keying material at any time necessary (availability); that the key management service allows nodes to obtain keying material from other network nodes while having the ability to authenticate its validity (authentication); and that the keying material supports the use of data encryption schemes to ensure that only the communicating parties are able to understand the transmitted data (data confidentiality), integrity schemes to ensure transmitted data is secure against modification (data integrity), and signature schemes to prevent a party from denying that it transmitted the data (non-repudiation).

2) CONNECTIVITY

In this context, nodes are connected when they have a secure means of obtaining necessary keying material in a verifiable manner. Therefore, a network has a high connectivity rate when any arbitrary set of network nodes have a high probability of obtaining each other's keying material in a verifiable manner. Additionally, connectivity is an important requirement for network operators to consider if they are interested in utilizing network coding while preventing data pollution attacks.

3) OVERHEAD

The overhead requirement encompasses the communication overhead, the computational overhead and the memory storage overhead. An efficient key management scheme minimizes the overhead without compromising any of the other requirements. The computational capabilities and the memory storage volume of mobile devices continues to improve and is expected to keep improving over time. Due to this ongoing development, these constraints are not considered as highly impactful. Therefore, key management schemes are mainly evaluated based on their communication overhead.

4) SCALABILITY

Due to the network architecture being designed to serve an urban landscape, it is considered that mobile small cells have the capacity to contain large numbers of mobile devices. However, the size of a mobile small cell is yet undefined and will therefore not be bounded in any of the considered key management schemes. Also, over time mobility causes the number of users inside a mobile small cell to fluctuate. The key management scheme must therefore be both scalable in terms of efficiently supporting a large fixed network size while also supporting dynamic network size changes.

5) SUSTAINABILITY

The 5G and beyond 5G mobile network is considered to have a long lifetime. Designed key management schemes must be

able to provide key management services from a security, connectivity and overhead perspective. This means that the key management scheme must resists any malicious attack for which the attacker has an extended time to make its attack successful, it is able to maintain a high level of connectivity and the overhead does not grow based on events happening over time. If a key management scheme is able to perform these tasks for the entire lifetime of the network, then the scheme is considered sustainable.

6) FAIRNESS

Fairness implies that the overhead costs to establish and maintain proper key management are fairly distributed over all the network nodes throughout the entire lifetime of the network. When the fairness requirement is not met, device owners are more likely to behave selfishly (i.e. free-riding behavior) and make their device unavailable to route data. This reduction in availability indirectly reduces connectivity and increases the overhead cost per node.

7) SECURE ROUTING INDEPENDENCE

This requirement relates to the secure routing interdependency problem [43], [44]. Secure routing protocols, such as [45]–[50] were developed for wireless ad hoc networks and they rely on a pre-established and underlying key management scheme to securely route data through the network. Therefore, when a key management scheme wishes to utilize a secure routing protocol to securely distribute keys, we reach an impasse. Thus, it is important that a key management scheme does not rely on secure routing [51], [52].

C. NOTATION

This article has limited the amount of variables, parameters and symbols in the text by not including details of the key management approaches such as algorithms, equations and protocols. These details are omitted since their impact on the evaluation for adoption is negligible. The variables, parameters and symbols which are used throughout this article are provided in Table 2.

TABLE 2. Variables, parameters, and symbols.

Symbol	Description
N_i	Network node i.
S_i	Server node i.
ID_i	The identity of node i.
n	The number of nodes in a network.
t	The threshold value of a threshold cryptography scheme.
MPK	The master public key.
MSK	The master private key.
pk_i	The public key of node i.
sk_i	The private key of node i.
ppk_i	The partial public key of node i.
psk_i	The partial private key of node i.
s_i	The secret share of node i.
$\|\|$	The concatenation of values.

IV. CERTIFICATE-BASED KEY MANAGEMENT SCHEMES

In certificate-based public key cryptography (CB-PKC), every node inside a network can generate their own public and private key. These public and private keys are mathematically linked which allows them to be used for various cryptographic protocols, such as the creation of unforgeable signatures, the verification of these signature, the encryption of data or the decryption of encrypted data. However, public keys being distributed between nodes inside such a network must be linked to its owner and be verifiable. Typically, a node would contact a TTP – also known as a Certification Authority (CA) – which verifies the identity of the node. After verification, the CA creates a certificate for this node, containing the nodes' identity, its public key and an unforgeable signature. The node is now able to distribute this certificate to other nodes inside the network, which are able to verify the authenticity of the certificate from the signature provided by the CA. This CA is an online central control point, which does not fit in a network of mobile small cells. The authentication of public keys therefore requires an alternate mechanism.

This chapter discusses five key management approaches relying on CB-PKC. The certificate chaining-based approach, the mobility-based approach, the self-certification-based approach, the partially distributed CA-based approach and the fully distributed CA-based approach.

A. CERTIFICATE CHAINING-BASED KEY MANAGEMENT

The certificate chaining-based approach was introduced by Hubaux *et al.* in [53], and later fully described by Capkun *et al.* in [54].

1) SYSTEM OVERVIEW

This approach relies on network nodes establishing a web-of-trust, similar to the e-mail security system Pretty Good Privacy (PGP) [55], which allows for the authentication of every node's public key. The basic idea is that nodes which have a pre-existing trust relationship uses this trust to sign each other's certificates, containing the node's identity and its public key. Suppose that nodes *A* and *B* trust one another and decide to issue each other's certificates. Both nodes create a certificate for each other and exchanges these while also keeping a copy of the certificate for their personal certificate repository. Suppose that nodes *B* and *C* also have a trust relationship and decide to issue certificates for each other. When node *A* and *C* wish to communicate, without having a pre-existing trust relationship, they merge their personal certificate repositories in order to look for a chain of trust connecting both nodes. Since node *A* trusts node *B* and node *B* issued a certificate for node *C*, node *A* has reason to believe that this certificate contains node *C*'s authentic public key. However, when no chain of trust exists between both

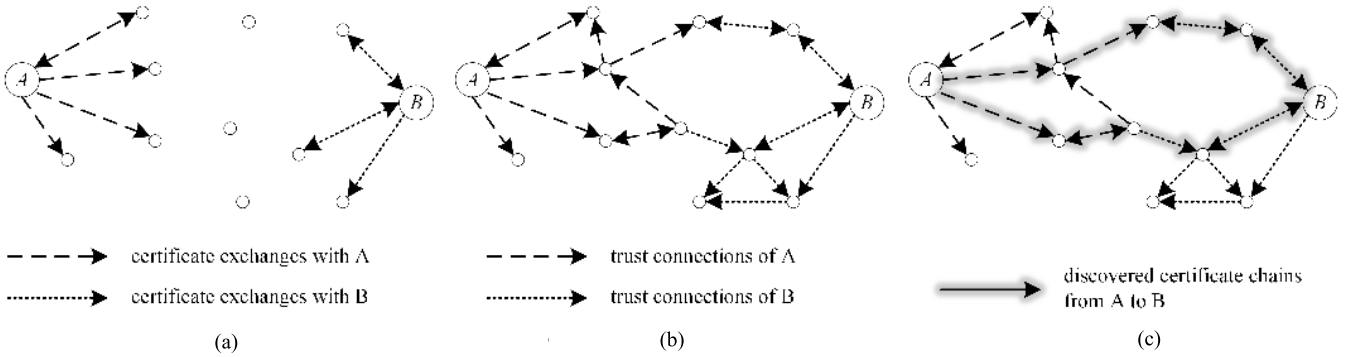

FIGURE 3. Illustration of three main phases in the certificate chaining-based approach. (a) Certificate issuing phase. (b) Certificate exchange phase. (c) Certificate chain discovery phase.

nodes after merging their personal certificate repositories, they have no reason to trust the authenticity of exchanged certificates.

2) SYSTEM DETAILS

This system consists of five main phases. The network initialization phase, the certificate issuing phase, the certificate exchange phase, the certificate repository update phase, and the certificate chain discovery phase. In the first phase, the network initialization phase, every node wishing to be a part of the network creates their own public-private key pair. To establish some initial trust and connectivity in the network, [56] proposed to have a trusted secret dealer distribute identities and public keys of k arbitrary nodes to each network node. The following four phases are performed throughout the entire lifetime of the network.

In the second phase, the certificate issuing phase, nodes issue certificates to neighboring nodes. When node A believes that the presented public key belongs to node B, it will issue a certificate. This certificate includes the identity of node B, its public key, the time of certificate issuing and the time of certificate expiration along with the signature of node A. Node A transmits this certificate to node B while also keeping a copy. These certificates are stored in the node's local certificate repository. Trust relationships between nodes can be displayed in a trust graph as shown in Fig. 3(a). This is a directed graph in which the vertices represent the public keys of nodes and the directed edges represent the issued certificates verifiable by the node's public key. There is a directed edge from vertex A to vertex B when node A issued a certificate for node B.

In the third phase, the certificate exchange phase, neighboring nodes exchange certificates. Obtained certificates are stored into the node's local certificate repository. This certificate exchange mechanism creates awareness of trust relationships in the neighborhood and is illustrated in Fig. 3(b). Node mobility forces this certificate exchange mechanism to be performed periodically. Instead of exchanging certificates, [57], [58] proposed to exchange simple trust relationship information to reduce the storage requirement. Certificates would only be exchanged on-demand to establish a certificate chain. The certificate exchange phase could even be entirely removed [59]–[67] and instead have on-demand routing protocols, such as ASNS [61]–[63], DSR [68] or AODV [69], find certificate chains. However, these schemes increase delay and communication overhead.

In the fourth phase, the certificate repository update phase, nodes update their local certificate repositories. Due to the limited amount of storage, the most recent certificates are kept in storage and nodes update their respective trust graphs accordingly.

In the fifth phase, the certificate chain discovery phase, nodes wishing to securely communicate attempt to discover a certificate chain. Suppose that node A wishes to communicate with node B, then node A first examines its local certificate repository for a certificate chain connecting both nodes. If node A is unable to find a certificate chain, then node A contacts node B and requests its local certificate repository. Node A merges both certificate repositories in order to find a certificate chain. This process is synonymous to merging both nodes' trust graphs to find a path connecting both nodes and is illustrated in Fig. 3(c). Once node A finds a certificate chain, it verifies the validity of each certificate to eventually verify the validity of the public key of node B. Hubaux *et al.* [53] proposed two algorithms to find a certificate chain. To simplify the certificate chain discovery process, [70]–[72] proposed the use of a cluster-based hierarchy while [73]–[75] proposed the use of a (binary) tree-based hierarchy. In case multiple certificate chains are discovered, [64], [66], [70], [71], [76]–[79] proposed various methods of adding a continuous trust metric to links in order to select the most trustworthy certificate chain. According to [80], some threshold amount of chains resulting in the same public key should exist before it can be considered trustworthy.

Capkun *et al.* [54] described three scenarios in which certificates are revoked. In the first scenario, a certificate reaches its expiration time. In this case, nodes move this certificate from its local certificate repository to a non-updating certificate repository. To prevent certificates from expiring, nodes within communication range of their certificate issuer can request a new certificate. In the second scenario, nodes are

allowed to revoke any certificate they previously issued when they believe that the binding between the node's identity and its public key is no longer valid. In the third scenario, a node believes that his private key has been compromised. This node contacts nodes which issued a certificate to it and requests them to revoke these certificates. The created revocation statements will spread through the network during the certificate exchange phases. To more rapidly spread certificate revocation information, [59], [60] proposed to broadcast these statements immediately to all two-hop neighbors.

To increase the security of this system, [67], [77], [79], [81], [82] proposed to combine certificate chaining with a partially distributed certificate authority (PD-CA) which acts as a trust anchor. More details about the PD-CA-based key management approach can be found in section IV-D.

3) EVALUATION FOR MOBILE SMALL CELLS

The security requirement is not met due to the reliance on the assumption that trust is transitive while this is not necessarily the case [83]. Node A may trust node B and node B may trust node C, but node A may not necessarily trust node C. Furthermore, trust is context-dependent [84]. Node A may trust node B as a sports coach, but not as a security expert. A malicious user may abuse his trust relationships to disrupt communication. Furthermore, the certificate issuing process is assumed to be performed physically to prevent malicious MITM attacks. Seeking physical contact to issue certificates is unrealistic in our scenario architecture and requires an alternative approach.

The connectivity requirement is not met either. To establish secure communication between an arbitrary set of nodes, there must be a high probability that a certificate chain exists. This key management approach was proposed for MANETs for use cases such as military and rescue operations. In both cases, network nodes consist of users with many pre-established trust relationships. This creates clusters of trust relationship while inter-cluster relationships are established by cluster-heads cooperating to achieve their common goal. This translates to a network with a high certificate-density and therefore a high probability of establishing a certificate chain between an arbitrary set of nodes. The network of mobile small cells consists of users with fewer pre-established trust relationships. The certificate-density is therefore lower, reducing the chances of nodes establishing a certificate chain. Distributing keying information from a trusted dealer during the network initialization phase could improve connectivity [56], however this will have a reduced effect over time.

The secure routing independence requirement is not met either. The exchange of certificate repositories seems to rely on secure routing to counter MITM attacks.

No issues have been identified related to the overhead, scalability, sustainability and fairness requirement. Based on these evaluations, the authors believe that the certificate chaining-based key management approach will not be able to provide efficient and effective key management to support cryptographic protocols and secure a network of mobile small cells.

B. MOBILITY-BASED KEY MANAGEMENT

The mobility-based key management approach was introduced by Capkun *et al.* in [85], [86].

1) SYSTEM OVERVIEW

This approach uses network mobility to its advantage. To establish secure communication, this approach proposes that nodes initially meet physically in order for both to verify each other's identity. Both nodes would exchange keying information (i.e. issued certificates) with their mobile devices using a short range communications system (e.g., infrared or wire). It is assumed that the exchange over this secure side channel is activated by both nodes simultaneously and consciously. By having short range entity authentication, some of the classical 'remote' entity authentication problems like identity impersonation and Sybil attacks [87] are prevented. Friends, family members and colleagues (users with a bi-directional trust relationship) inside this network would similarly exchange keying information offline or over the secure side-channel. Simulations in [85] show that a reasonably long time is required before sufficient connections are made to establish reliable communication inside this network. To reduce this problem, they proposed that nodes sharing a common friend can use that relationship to obtain trustworthy keying information. This information can be transmitted remotely since both nodes previously established a secure channel with their friend. These simulations also show that the use of the common friend mechanisms, to further distribute keying information, can reduce the convergence time of reliable network communication by a factor of 10.

2) SYSTEM DETAILS

This system consists of three main phases. The network initialization phase, the certificate issuing phase, and the certificate exchange phase. In the first phase, the network initialization phase, every node wishing to be a part of the network creates their own private key and the corresponding public key. The following two phases are performed throughout the entire lifetime of the network.

In the second phase, the certificate issuing phase, network nodes exchange their public keys to each other in order to issue and exchange certificates in the next phase. Due to network mobility, nodes will physically meet every so often. Meeting nodes which do not have any prior trust relationship provide identifying information in order to prove their identity to the other. If both nodes are convinced that the other node's public key belongs to the provided identity, they use the short range and secure side channel (i.e. over infrared or wire) to exchange keying information on their mobile devices. This side channel ensures data integrity by eliminating any active adversary. A series of exchanges provide both nodes with each other's public key and a signature to prove that the other node has the private key corresponding to

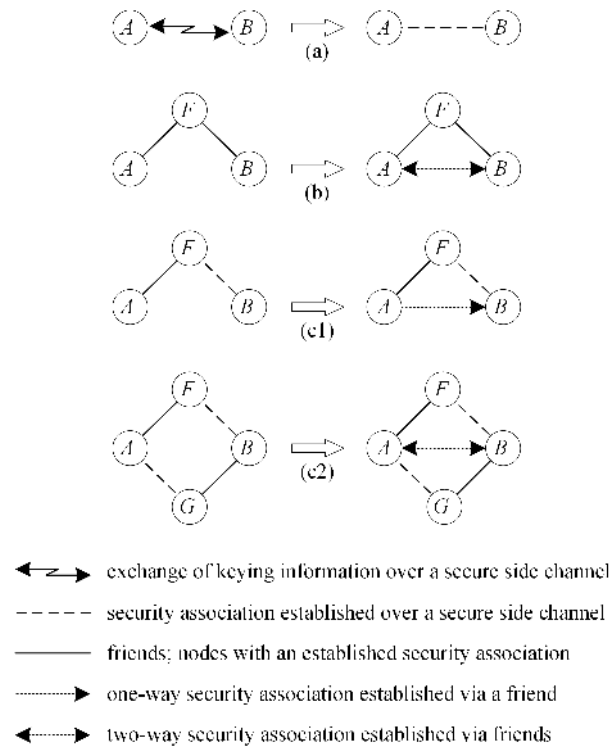

FIGURE 4. Mechanisms to establish security associations between network nodes in the mobility-based approach.

the public key. This provides both nodes with a secure communications channel, displayed as mechanism (a) in Fig. 4. Details of the keying information exchange protocol can be found in [86]. Nodes which have an existing bi-directional trust relationship are called friends and they can similarly use the secure side channel to exchange their public keys.

In the third phase, the certificate exchange phase, network nodes distribute certificates. In mechanism (b) of Fig. 4, two nodes A and B share a common friend F. Since friend F previously exchanged its public key with both node A and node B, it can issue fresh certificates on request and transmit these to both nodes. Both node A and B are able to verify the certificate provided by F, since they both trust F and have the their friend F's public key. Mechanisms ($c1$) and ($c2$) in Fig. 4 are combinations of mechanism (a) and (b). In mechanism ($c1$), node A has a friend F, who previously exchanged keying information with node B. On request from node A, friend F could issue a fresh certificate of node B's public key and transmit this to node A. Since node A exchanged public keys with friend F, and also trusts friend F, it can verify the authenticity of node B's certificate. However, node B exchanged public keys with node F after meeting physically which led node B to believe that the public key of node F is authentic. Node B has no further trust relationship with node F, and therefore will not consider certificates coming from and signed by node F to be trustworthy. Mechanism ($c1$) therefore only provides a uni-directional security association. Mechanism ($c2$) is a further expansion of mechanism ($c1$) in which, using the same logic as before, can provide a bi-directional security association between nodes A and B. According to simulations, the common friend mechanisms further distribute keying information almost by a factor of 10. To provide data integrity, [88] proposed the use of hash functions in the creation of security associations such that chains of trust can be established which are longer than just 2 links.

Capkun *et al.* [85], [86] also provide a symmetric key management variety. Instead of having a common friend which distributes signed certificates, the friend would act as a trusted entity to provide both of its friend nodes with a shared symmetric key. This shared symmetric key could be generated by the common friend and distributed to both nodes (like in the Kerberos protocol [89]) or one of the two nodes would generate a symmetric key and the common friend would relay it to the other node (like in the Wide-Mouthed-Frog protocol [90]).

No details are provided about certificate revocation.

3) EVALUATION FOR MOBILE SMALL CELLS

The security requirement is conditionally met. Similar to the certificate chaining-based key management approach, three mechanisms are proposed which rely on transitive trust which is not necessarily secure [83], [84]. This scheme is still more secure compared to the certificate chaining-based approach since the number of trusted entities involved in exchanging keying information is limited to one. Nevertheless, explicit security can only be guaranteed by omitting mechanisms (b), ($c1$), and ($c2$) illustrated in Fig. 4. The disadvantage is that reliance on only mechanism (a) further disconnects the network. Furthermore, the physical contact required to set up security associations is unrealistic in our scenario architecture and requires an alternative approach.

The connectivity requirement is not met either. To establish secure communication between an arbitrary set of nodes, there must be a high probability that these nodes can establish security association with each other. However, connectivity in this approach relies on the mobility intensity and the validity period of issued certificates. As network nodes become increasingly mobile, they meet nodes more often and can establish more security associations. A longer validity period also increases the amount of valid security associations, unfortunately this also comes at the cost of an increased memory overhead. Furthermore, this approach is limited when it comes to connectivity in comparison to the certificate chaining-based approach which can establish security associations through friends-of-friends and beyond. A small network may be able to provide a sufficient level of connectivity, but this is not expected for a network covering the urban landscape.

No issues have been identified related to the overhead, scalability, sustainability, fairness and secure routing independence requirement. Based on these evaluations, the authors believe that the mobility-based key management approach will not be able to provide efficient and effective key management to support cryptographic protocols to secure a network of mobile small cells.

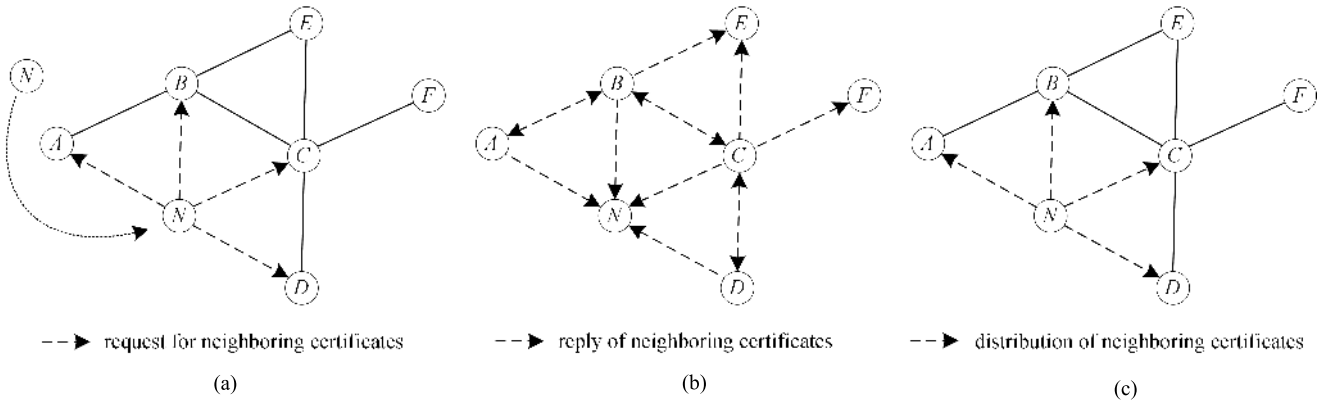

FIGURE 5. Illustration of the neighborhood certificate distribution mechanism in the self-certification-based approach. (a) node N requests certificate distribution (b) neighboring nodes A,B,C, and D reply (c) node N finalizes the distribution.

C. SELF-CERTIFICATION-BASED KEY MANAGEMENT

The self-certification-based key management approach was introduced by Li *et al.* [91].

1) SYSTEM OVERVIEW

In this approach network nodes issue their own certificates. Upon nodes joining the network or moving into a new neighborhood, nodes broadcast a request for certificate distribution (while also sending their own certificate) to everyone within their transmission range, also called their 1-hop neighborhood. Every 1-hop neighbor responds by broadcasting the certificates of all of its 1-hop neighbors. This certificate distribution mechanism provides the newly moved-in node with certificates from all nodes within its 2-hop neighborhood. At the same time, neighborhood monitoring prevents nodes from sending false certificates. Suppose that a node has been compromised and sends a false certificate during the certificate distribution process, neighboring nodes can detect this false transmission. These neighboring nodes possess the certificates of their 2-hop neighbors and can therefore cross-check if a compromised neighbor sends any false certificates. A node wishing to communicate with another node within its 2-hop neighborhood can use the certificate provided during the certificate distribution. If the two nodes are more than two hops away from each other and do not share each other's certificate, they can request a multi-hop certificate distribution. This multi-hop certificate distribution basically floods the network in search for the node that the requester wishes to communicate with and through chains of certificates, which are verified at every step against malicious users, a route can be established to share verified certificates and therefore the public keys of each other.

2) SYSTEM DETAILS

This system consists of three main phases. The network initialization phase, the neighborhood certificate distribution phase, and the multi-hop certificate distribution phase. In the first phase, the network initialization phase, every node wishing to be a part of the network creates their public-private key pair followed by a self-issuing of its certificate. This is the creation of the certificate by the node itself in which it signs it own certificate. The signature is created from the node's private key and the hashed information on the certificate such that any other node can verify that the certificate is created with a valid public-private key pair. The following two phases are performed throughout the entire lifetime of the network.

In the second phase, the neighborhood certificate distribution phase, nodes broadcast certification information upon neighborhood changes. Every node in the network periodically broadcasts *hello*-messages to inform other nodes of their 1-hop neighbors. When a node N joins a new neighborhood, a 3-step neighborhood certificate distribution process is triggered. This process is illustrated in Fig. 5. In the first step, the node N broadcasts a request for certificates of its neighbors, while distributing its own certificate. In the second step, neighboring nodes receiving the request verify the received certificate for authenticity. Upon correct verification, the node replies by broadcasting a message containing its own certificate and the certificates of its 1-hop neighbors. This informs the 2-hop neighbors of node N joining the neighborhood while also informing the node N about its 2-hop neighbors. Finally, node N broadcasts a message containing its certificate and the certificates of all its 1-hop neighbors. This is necessary since node N may have created a 2-hop connection between nodes which previously did not exist. Nodes perform neighborhood monitoring during this phase. Since every node is aware of their 2-hop neighbors, they are able to cross-check if every neighbor broadcasts the correct certificates of its 1-hop neighbors.

The third phase, the multi-hop certificate distribution phase, is triggered when a node A wishes to establish a connection with a node B and are separated by more than two hops. Node A broadcasts a request message containing its own certificate and the identity of node B. The 1-hop neighbors verify node A's signature after which they append the request message with their own certificate and a signature of this extended request message. Then, these 1-hop

neighbors broadcast the extended request message further along the network. The 2-hop neighbors and subsequent neighbors verify the signature from the previous two nodes and continue this process. Verification is necessary to detect any malicious behavior. Nodes drop any returning requests such that the request message travels from node A to its 1-hop neighbors, 2-hop neighbors, and so on, until it reaches node B. This mechanism prevents a Sybil attack [87].

If a node believes that its public-private key pair is compromised, it can select a new private key with its corresponding public key and create a self-issued certificate. Also, when a node's certificate expires it can self-issue a new certificate. The node then broadcasts a certificate revocation message consisting of its old certificate, its new certificate, and a signature. The 1-hop neighbors will verify this message and broadcast it to inform the 2-hop neighbors. There is no mention of a particular mechanism which reports malicious activities discovered from neighborhood monitoring.

3) EVALUATION FOR MOBILE SMALL CELLS

The security requirement is not met. This is due to the key management approach being outright vulnerable to an impersonation attack caused by self-certification. Li *et al.* [91] points out that nodes inside the network which have previously exchanged the certificate of the real node have its certificate stored in their certificate table and could therefore detect malicious behavior over time. However, the impersonator could cause major damages by the time this is detected and reported. This impersonation attack is claimed to be preventable by creating a strong one-to-one binding between the certificate and the public key of the user [92]. The viability of this solution requires further investigation.

The overhead requirement is not met either. Due to this approach relying on nodes being constantly aware of their 2-hop neighborhood to provide proper neighborhood monitoring and the network of mobile small cells being proposed for an urban environment with a constantly changing network topology, nodes are required to broadcast *hello*-messages with rather short intervals. This causes a large communication overhead.

The scalability requirement is not met. An increase in network density would indicate more topological changes which further increases the communication overhead. Also, an increase in network range (i.e. a larger portion of nodes are more than 2 hops away from each other) would increased the use of the multi-hop certificate distribution which relies on flooding the network with broadcast messages in order to find the requested certificate and public key. This scheme is therefore not scalable from an overhead perspective.

No issues have been identified related to the connectivity, sustainability, fairness and secure routing independence requirement. Based on these evaluations, the authors believe that the self-certification-based key management approach will not be able to provide efficient and effective key management to support cryptographic protocols to secure a network of mobile small cells.

D. PARTIALLY DISTRIBUTED CA-BASED KEY MANAGEMENT

The partially distributed CA-based approach (PD-CA) was introduced by Zhou *et al.* in [93]. This approach distributes the trust from an ordinary centralized CA to a proper subset of network nodes and is therefore called partially distributed. Zhou *et al.* implemented their online distributed CA [94], [95] although not in an ad hoc environment.

1) SYSTEM OVERVIEW

The general idea of the PD-CA-based key management approach is distributing the trust from a single centralized trusted authority to a proper subset of nodes inside the network. This subset of nodes, called servers, perform the certifying tasks collectively. Upon network initialization, a master public-private key pair is created. The master public key is made public while the master private key is divided into n shares and distributed to the n servers. These shares are created from a t-out-of-n threshold cryptography scheme [96], [97]. In this key management scheme, a threshold of at least t trustworthy servers is required to create a valid signature on a certificate. An adversary needs to compromise at least t servers to be able to reconstruct the master private key such that it can create false signatures. To prevent this from happening, [93] proposed to combine their scheme with proactive threshold cryptography [98]–[102] and verifiable threshold cryptography [103], [104]. Proactive threshold cryptography includes periodic share refreshing which means that an adversary is required to compromise at least t servers before these shares refresh. Verifiable threshold cryptography includes a method of verifying the correctness of shares such that a compromised server can be detected when its incorrect share is used in an attempt to create a valid signature.

2) SYSTEM DETAILS

This system consists of three main phases. The network initialization phase, the certificate issuing phase, and the share updating phase. In the first phase, the network initialization phase, an offline trusted authority creates a master public-private key pair. The master public key is made public and the master private key is divided into n shares using a (n, t) proactive threshold cryptography scheme [98]–[102]. The shares are then distributed to n nodes inside the network which will function as the distributed CA. These nodes are called servers. This process is illustrated in Fig. 6(a). Zhou and Haas [93] did not mention a method for selecting servers, however [105]–[111] proposed to select servers based on physical security and computational ability, [112], [113] proposed to select servers which have a high success ratio of providing key management services, and [114], [115] proposed to select the maximum clique in a trust graph as servers. Each server stores the public keys of all the nodes in the network, including the other servers, so they have a secure channel. Every node wishing to be part of the network creates their own public-private key pair. The

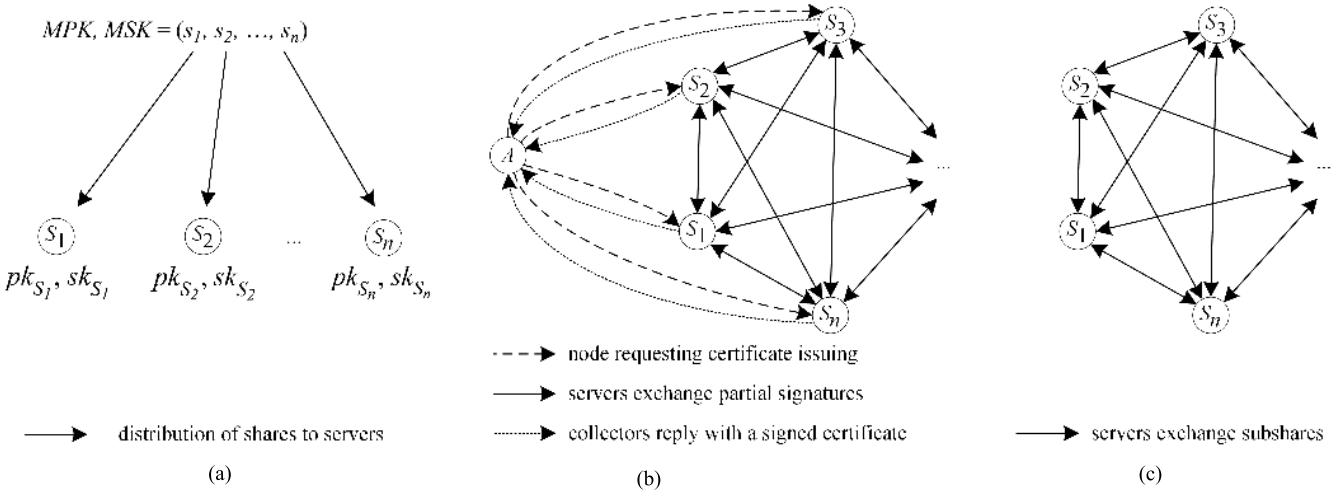

FIGURE 6. Illustration of the three main phases in the partially distributed certificate authority-based approach. (a) Network initialization phase. (b) Certificate issuing phase. (c) Share updating phase.

following two phases are performed throughout the entire lifetime of the network.

In the second phase, the certificate issuing phase, nodes wishing to be part of the network or nodes whose certificate is soon to expire contact at least t servers to issue a certificate. To contact t servers, it is assumed that [93] would resort to flooding the network with certificate issuing requests. To reduce delay and communication overhead, [105]–[108] proposed to use cached routing information and [110], [111] proposed to have the servers form a multicast group such that a requesting node only requires to contact a single (uncompromised) server. Nodes provide the servers with identifying information and their public key. Then each server creates a partial signature and sends this to a so-called combiner. Any server can act as a combiner and Zhou and Haas [93] proposed to have t servers act as combiners to create at least one valid signature in the presence of compromised servers. After a combiner receives t partial signatures, it combines these into a certificate signature. The combiner can verify its correctness with the public master key before transmitting it to the requesting node. This process is illustrated in Fig. 6(b). To reduce the communication overhead of the servers, [105]–[111] proposed to have servers transmit the partial signatures directly to the requesting node which combines these into its signed certificate. The use of self-certifying keys [116] was proposed in [117] since these require nodes to contact servers only once.

In the third phase, the share updating phase, servers update their individual shares to prevent mobile adversaries [118] from collecting t shares. Each server creates subshares which it distributes to the other servers. Then, each server combines their original share with the received subshares to create a new share. This new share is independent of the previous share, meaning that a mobile adversary is unable to use previously obtained shares to reconstruct the master private key. This process is illustrated in Fig. 6(c). Algorithms for periodic share updating and share updating due to servers leaving and/or joining the server group are provided in [110], [111], [119].

The certificate revocation mechanism in [108] proposed that servers create partially signed revocation certificates and broadcast these through the network using flooding. These partial revocation certificates are stored locally in each node's certificate revocation list (CRL). When a node receives t partially signed revocation certificates, it creates the fully signed revocation certificate which is then accepted as legitimate. Alternatively, [110], [111] proposed that nodes report misbehavior to the multicast server group. At least some threshold u accusations (from u nodes) are required in order to revoke a node's certificate. Revoked certificates are periodically broadcasted and locally stored on a node's CRL. The identity of accusers is also stored at servers to track any false accusers. To measure trust of individual nodes, [120], [121] proposed the use of a Trust Management system which decides whether a node is trustworthy enough to receive key management services. This trust is measured by the node's success rate of transmitting data during its lifetime in the network.

To increase scalability and improve availability by distributing the servers evenly, [122] proposed to have the network partitioned into clusters such that each cluster-head maintains the cluster structure and acts as a server of the PD-CA. This inspired more research into a PD-CA with a clustered architecture [123]–[128]. To reduce the memory storage requirement, [129]–[132] proposed key management schemes relying on elliptic curve cryptography (ECC) [133].

3) EVALUATION FOR MOBILE SMALL CELLS

The security requirement is met since the offline TTP distributes shares which provide trustworthiness in the collectively signed certificates. Verifiable threshold cryptography allows the detection of malicious behavior and proactive threshold cryptography provides robustness against mobile

adversaries. However, a node wishing to join the network could be vulnerable to a MITM attack [134]. A malicious node could provide the joining node with a false master public key for which the malicious node has the corresponding master private key. Fortunately, this attack can be prevented when at least t combiners transmit the master public key along with the signed certificate.

The overhead requirement is not met. The expensive certificate management and certificate distribution in this PD-CA-based approach is believed to cause a large communication overhead for a moderate to large network which covers the urban landscape.

The scalability requirement is not met either. The scalability of the network is strongly related to the number of servers acting as the distributed CA since these servers must provide all network nodes with certification services. A growth in the number of network nodes increases the pressure on these servers and subsequently reduces its battery life. For mobile small cells it is reasonable to assume that the number of nodes fluctuate over time and could drastically increase in certain areas during sporting events, concerts and national celebrations. The limited amount of servers could become incapable of providing key management services at this point. This scheme is therefore not scalable from a connectivity perspective. Temporary on-demand auxiliary servers, proposed in [109], [135], may be able to reduce the severity of this problem.

The sustainability requirement is met. Although it is reasonable to assume that the assigned servers acting as a distributed CA may leave the network at some point, resulting in an unavailable key management service followed by a disconnected network, a solution to this problem has been proposed. The key management scheme [136] is also based on a partially distributed authority (although based on certificateless PKC) and proposed a mechanism to replace a server node in the event that one would leave the network. Due to the similarities of the key management structure, it is assumed that this mechanism can be easily adopted in the PD-CA-based approach. This approach is therefore sustainable from a connectivity perspective. Furthermore, an extensive network lifetime does not improve the abilities of adversaries to break security or worsen issues related to overhead.

The fairness requirement is not met due to the imbalance of overhead between network nodes. Even if servers are replaced periodically in an attempt to fairly distribute the key management tasks and its associated overhead over time, user's mobile devices which are temporarily assigned as a server may still choose to act selfishly.

No issues have been identified related to the connectivity and secure routing independence requirement. Based on these evaluations, the authors believe that the PD-CA-based key management approach will not be able to provide efficient and effective key management to support cryptographic protocols to secure a network of mobile small cells.

E. FULLY DISTRIBUTED CA-BASED KEY MANAGEMENT

The fully distributed CA-based approach (FD-CA) was introduced by Luo *et al.* in [137]. This approach distributes the trust from an ordinary centralized CA evenly among all the network nodes and is therefore called fully distributed. This approach was later simulated and implemented in [138]–[140].

1) SYSTEM OVERVIEW

Similar to the PD-CA-based key management approach, the general idea is to distribute trust from a single centralized trusted authority to a set of network nodes due to MANETs being unable to support a centralized CA. In this FD-CA-based key management approach, trust is distributed among all the nodes. It is assumed that each node has some one-hop neighborhood discovery mechanism and that they have at least t one-hop neighbors at any time. Upon network initialization, a master private key and the corresponding master public key are created. The master public key is made public to all network nodes while the master private key is divided into t shares and distributed to a cluster of t neighboring nodes. The cluster of t neighboring nodes, each in possession of a share of the master private key, is able to collaboratively create new shares for its one-hop neighbors. This mechanism is used to spread shares to all the nodes inside the network in a scalable manner. It is also used to provide nodes with a share when they join the network. Similar to the PD-CA-based approach, proactive threshold cryptography [98] and verifiable threshold cryptography [103], [141], [142] are combined to create, verify, and update shares in order to provide robustness against mobile adversaries [118] and DoS attacks. Each node creates their own private and corresponding public key after which they broadcast a request to their neighboring nodes to have its public key certified. When the node receives $t-1$ responses of partial signatures, it combines these with its own share to create a new fully signed certificate. Any node requesting its certificate can verify its authenticity with the master public key and can therefore be safely distributed through the network. This proposal is designed to provide key management in wireless ad hoc networks which are dynamic, scalable and have a high node density.

2) SYSTEM DETAILS

This system consists of three main phases. The network initialization phase, the certificate renewal phase, and the share updating phase. In the first phase, the network initialization phase, an offline trusted authority creates a master private key (MSK) and the corresponding master public key (MPK). The master public key is made public and the master private key is divided into t shares using a t-out-of-t proactive threshold cryptography scheme [98]. These shares $(s_1, s_2, \ldots, s_t)$ are then distributed to a cluster of t neighboring nodes $(N_1, N_2, \ldots, N_t)$ inside the network. Nodes within broadcast range of at least t nodes with system shares, send a request to obtain their own system share. This system share is obtained

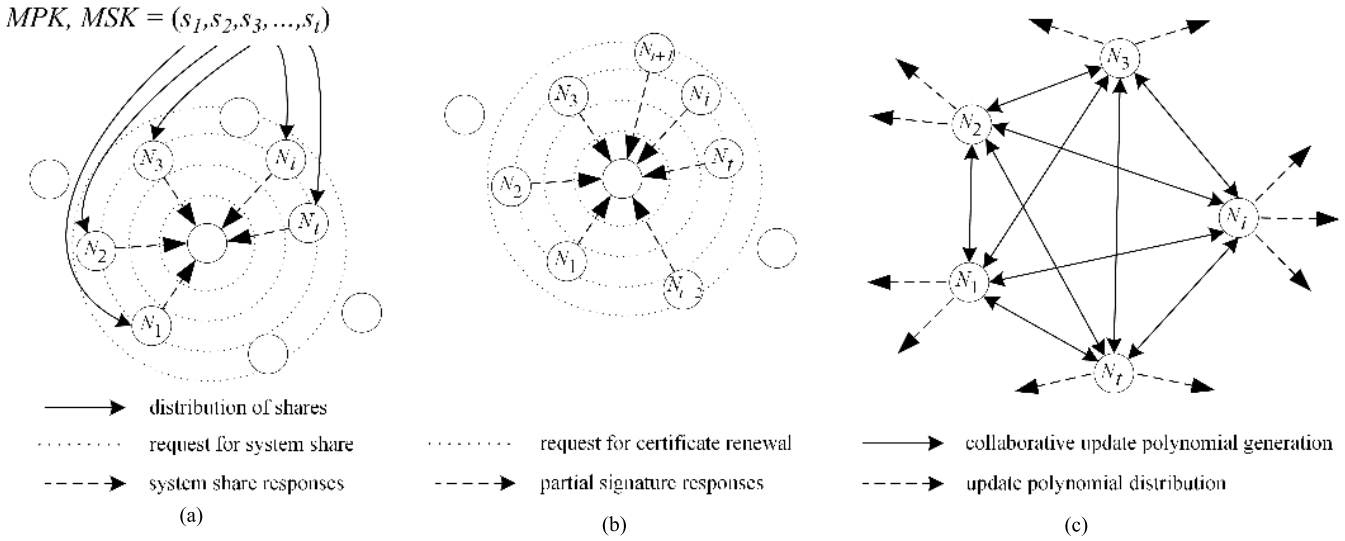

FIGURE 7. Illustration of the three main phases in the fully distributed certificate authority-based approach. (a) Network initialization phase. (b) Certificate renewal phase. (c) Share updating phase.

following the 2-round protocol described in [137], [138] and over time distributed to all the nodes inside the network. This process is illustrated in Fig. 7(a). During network operation, the same process is used to distribute a secret share to nodes joining the network. However, [143] demonstrated by example that the obtained secret share of a joining node is not verifiable. Various other schemes proposed to establish a cluster-based [144], [145] or a logical tree-based [146]–[148] hierarchy to organize the key management service. It is assumed that a node which joins the network already obtained an initial certificate, either from an offline authority or from a coalition of t networking nodes. The following two phases are performed sequentially throughout the entire lifetime of the network.

In the second phase, the certificate renewal phase, nodes whose certificate is soon to expire broadcast a request for a certificate renewal. It is assumed that each node is equipped with some detection mechanism to detect misbehaving nodes among its one-hop neighborhood. When neighbors receive the request and have no reason to believe that the requesting node is not a well-behaving node, it responds with a partial signature. This process is illustrated in Fig. 7(b). The requesting node can verify the correctness of the received partial signatures and combines t correct partial signatures to sign and renew its certificate. To reduce the computational overhead, [146] proposed the use of algorithms based on the discrete logarithm problem since these are more efficient than the originally proposed RSA-based algorithms.

In the third phase, the share updating phase, a random node creates a coalition of t nodes to initiate share updating. Luo and Lu [137] and Luo *et al.* [139] proposed a sequential process which is based on the share distribution during network initialization, and a parallel share update process. In the parallel share update process the coalition collaboratively generates, encrypts, and signs an update polynomial. This update polynomial is then distributed to all the nodes inside the network by flooding. This process is illustrated in Fig. 7(c). Each node receiving the encrypted and signed update polynomial can check its authenticity and decrypt it with the master public key. Then, each node sends a broadcast message requesting subshares from its one-hop neighbors. Upon receiving t valid subshares the node is able to update its master private key share. At the end of each share updating phase the old shares will be destroyed and the new shares are used to handle certificate renewal requests in the next certificate renewal phase.

Luo and Lu [137] and Luo *et al.* [139] assumed that each node is equipped with some detection mechanism to identify misbehaving nodes in its one-hop neighborhood. An example of a distributed detection mechanism is [149]. Each node maintains monitoring records on neighboring nodes and a certificate revocation list (CRL). Based on the monitoring records, a node may believe that a neighboring node is misbehaving. In this case, an accusation message is created, signed, and locally distributed. Each node receiving the accusation checks if they believe the accuser is to be trusted and if so, they create an entry in their CRL with the suspected node's ID and a list of its accusers. A total of t accusations are necessary to convict a node and therefore prevents a malicious node from falsely accusing and convicting a well-behaving node. Once a node is convicted, the t accusers create a signed conviction certificate and distributes this through the network. The extent of the conviction certificate distribution depends on the time that the convicted node's certificate is still valid. The distribution must cover enough nodes inside the network to prevent the convicted node from "escaping" to a new neighborhood to successfully renew its certificate before it expires. Nodes with expired certificates are believed

to be malicious and are unable to obtain a new certificate. Also, in order to minimize the storage requirement of the CRL it is proposed to remove entries of convicted nodes once their certificate has expired.

Various researchers proposed to make the threshold t dynamic to maximize the availability and security at any time. It is proposed to reduce the threshold value t when the network density decreases in order to keep certification services available [150], and to increase the threshold value t when the network density increases in order to provide security [151]. Alternatively, [152], [153] recognized that the FD-CA approach provides availability at the cost of security compared to the PD-CA approach and proposes a middle way in which nodes have duplicate secret shares.

3) EVALUATION FOR MOBILE SMALL CELLS

The security requirement is met since the offline TTP distributes shares which provide trustworthiness in the collectively signed certificates. Verifiable threshold cryptography allows the detection of malicious behavior and proactive threshold cryptography provides robustness against mobile adversaries. However, a node wishing to join the network could be vulnerable to a MITM attack [134]. A malicious node could provide the joining node with a false master public key for which the malicious node has the corresponding master private key. Fortunately, this attack can be avoided by having t well-behaving nodes transmit the master public key along with the partial signature since a mobile adversary is assumed to be incapable of simultaneously controlling t network nodes. Furthermore, the FD-CA-based approach is vulnerable to a Sybil attack [87]. In the Sybil attack a malicious user takes on multiple (in this case at least t) identities, thereby representing multiple nodes of which each has the ability to obtain a share derived from the master private key. For example, the malicious user could purchase t mobile devices and register these with different network providers in order to successfully register t devices and obtain t shares. This would allow the malicious user to recreate the entire master private key and break security within the system. This attack can be prevented by implementing policies, such as limiting the distribution of shares to one share per identity (which can be maintained through identity authentication) instead of one share per mobile device/SIM.

The overhead requirement is not met. The expensive certificate management and certificate distribution in this FD-CA-based approach is believed to cause a large communication overhead for a moderate to large network which covers the urban landscape.

No issues have been identified related to the connectivity, scalability, sustainability, fairness and secure routing independence requirement. Based on these evaluations, the authors believe that the FD-CA-based key management approach will not be able to provide efficient and effective key management to support cryptographic protocols to secure a network of mobile small cells.

V. IDENTITY-BASED KEY MANAGEMENT SCHEMES

Identity-based public key cryptography (ID-PKC) [38] was first proposed by Shamir in 1984, but it was not until 2001 when Boneh and Franklin [39], [40] introduced the first practical ID-based cryptosystem. This scheme was later extended by Lynn [154] to provide message authentication at no additional cost. This form of public key cryptography originated from the burden of obtaining authenticated public keys and the need to reduce the memory requirement from storing certificates. In ID-based cryptography, the identity (e.g., network address, phone number) is used to derive a node's public key. This information is already supposed to be known to a node wishing to communicate with another node. Therefore, this ID-based public key effectively removes the necessity to authenticate and distribute public keys. The private key is obtained from a trusted party called the Private Key Generator (PKG). This PKG combines a master private key with a node's identity to create that node's private key. However, this comes at the cost of having the PKG as a single-point-of-attack and it is capable of computing and storing every node's private key, also known as the key escrow problem. The obtained private key can be used to decrypt and sign messages. Suppose that node A wishes to send a message to node B. First, node A creates a message, encrypts its message with the identity of node B and then creates a signature using its own private key. Finally, node A sends the encrypted message, the created signature and its identity to node B. Node B can verify the signature with node A's identity, concludes that the message comes from node A and then decrypts the message with its private key.

This chapter discusses three approaches of establishing secure, efficient, and reliable key management initially designed for MANETs and relying on ID-PKC. The first approach (pre-distribution-based key management) includes an offline trusted authority which distributes keying material to network nodes prior to joining the network. The keying material includes both public and private keys which are used to establish secure communication channels between nodes in a scalable manner and minimizes communication overhead. The identity of nodes is used to derive which keys should be used in establishing secure communication. The following two approaches (partially distributed PKG-based key management and fully distributed PKG-based key management) provide private keys to network nodes by distributing the private key generating task of a centralized PKG to a subset or to all of the nodes inside the network.

A. PRE-DISTRIBUTION-BASED KEY MANAGEMENT

The pre-distribution-based key management approach was introduced by He *et al.* in [155], [156].

1) SYSTEM OVERVIEW

This approach utilizes combinatorics to distribute public and private keys while minimizing the memory storage requirement. In a typical network of n nodes, each node stores one

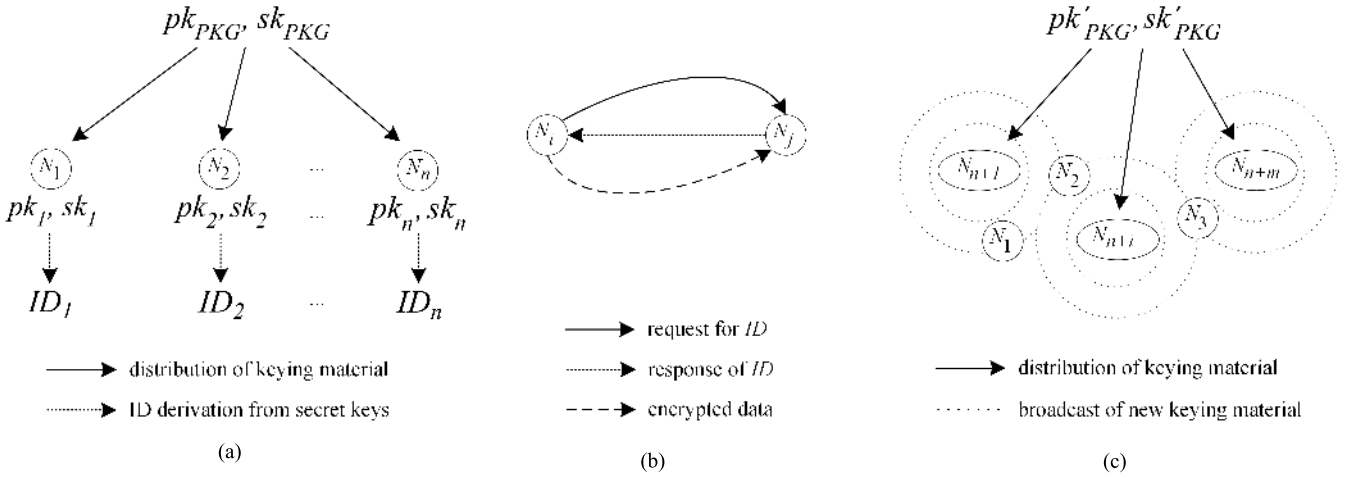

FIGURE 8. Illustration of the three main phases in the pre-distribution-based approach. (a) Network initialization phase. (b) Secure communication establishment phase. (c) New node joining phase.

private key and n public keys such that every pair of nodes have access to a secure communications channel. However, in such a key pre-distribution scheme the memory storage requirement grows linearly with the size of the network. In the approach introduced by He *et al.* [155], [156], a trusted authority generates a pool of public-private key pairs large enough such that every node will be provided with a unique combination of private keys. This trusted authority will be offline during network deployment. For example, a network of 10 nodes only requires 5 public-private key pairs. Prior to network deployment, each node will be provided with a unique combination of 2 private keys along with the entire pool of public keys. The memory storage requirement in this case is limited to 7 keys. The use of combinatorics to distribute keys means that the memory storage requirement only grows logarithmically and that makes this approach highly scalable. After a node receives its unique set of private keys, it derives its identity from the indexes of the received private keys. By exchanging identities between nodes, each node can derive which private keys another node has and uses the corresponding public keys to secure data. Only the intended node possesses the correct combination of private keys, providing security. When nodes wish to join the network, they would contact the trusted authority in an offline fashion to obtain their unique set of keys. If not enough unique combinations exist anymore, the offline authority generates additional keys. The additional keys will then be introduced into the network by the newly joining node, provided with a signature which could have only been created by the offline authority.

2) SYSTEM DETAILS

This system consists of three main phases. The network initialization phase, the secure communication establishment phase, and the new node joining phase. In the first phase, the network initialization phase, an offline PKG generates a pool of mathematically linked public and private key pairs. The size of this pool of keys is dependent on the number of nodes which are projected to be participating in the network. Suppose a network is projected to contain ten nodes. Instead of ordinarily providing each node with a single unique public-private key pair and nine public keys related to the remaining nine nodes, this scheme proposes the use of combinatorics to minimize the memory requirement. To accommodate ten nodes with keying material, only five public-private key pairs are necessary. Each node, before joining the online network, would receive a random and unique combination of two private keys along with the pool of five public keys from the PKG. This example effectively reduces the number of keys stored at a node from 11 to 7. The identity of the node is then derived from the indexes of the obtained private keys. Since the set of private keys is unique for every node, the identities will also be unique. This process is illustrated in Fig. 8(a). Notice that a node must use all of their private keys to sign or decrypt a single message to provide security. Algorithms provided in [155], [156] estimate the most optimal values for public-private key pool size and the number of private keys to be held by every node for an arbitrary network size while considering the objectives of memory efficiency, computational complexity and resilience requirement. To further reduce the memory storage requirement, [157], [158] proposed a clustering-hierarchy and requires nodes to only store the public keys of its cluster members. This only provides intra-cluster communication whereas inter-cluster communication has to be routed through the cluster-head. Also, cluster-heads are assigned to provide each cluster-member with appropriate keys upon dynamic member changes. This proposal fails the fairness requirement and causes additional communication overhead by trying to improving on an already low memory storage overhead.

In the second phase, the secure communication establishment phase, a node A wishes to communicate with another node B. First, the node A sends a message to request the identity of node B. Then, node B responds with its identity ID_B. Node A inspects the identity of node B and derives the indexes of the private keys that node B possesses. Node A uses the

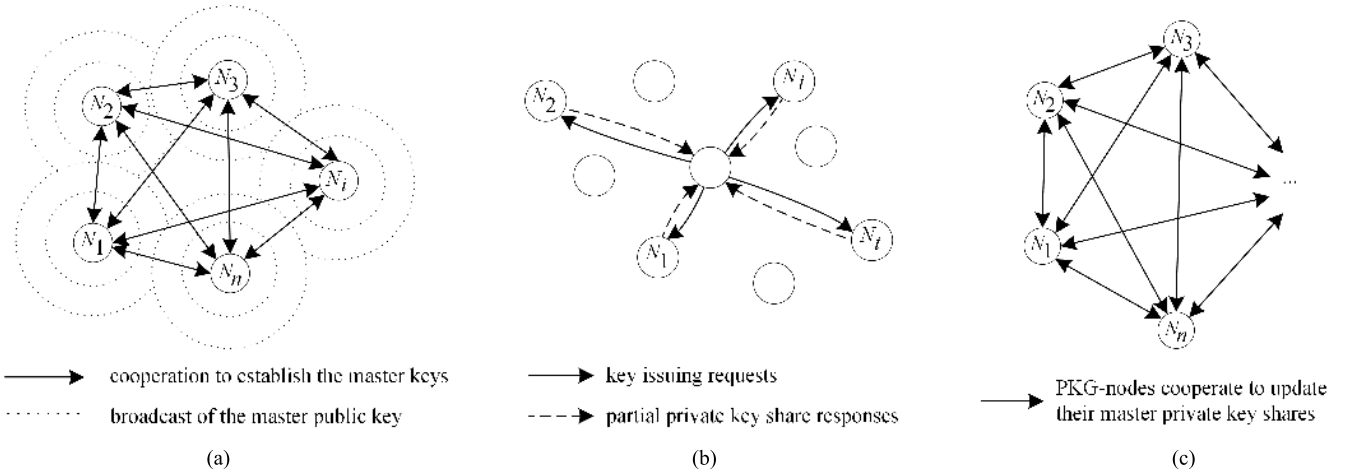

FIGURE 9. Illustration of the three main phases in the partially distributed private key generator-based approach. (a) Network initialization phase. (b) Private key issuing phase. (c) Share updating phase.

public keys corresponding to the private keys in possession by node B to encrypt its data and securely transmits this data. This process is illustrated in Fig. 8(b). He *et al.* [155], [156] proposed that each node its identity is a binary string of the indexes of the private keys it possesses. For example, the network of ten nodes has a total of five public-private key pairs. Suppose that a node received private key number 0 and private key number 3. It concatenates the binary values of these numbers to create its identity, in this case 000||011. Any other node wishing to securely communicate then uses public key number 0 and public key number 3 to encrypt its message. Since the identity of a node is used to establish secure communication, this key management approach is classified as an identity-based approach.

In the third phase, the new node joining phase, new nodes contact the offline PKG to obtain its keying material such that they can join the network. If there are still unused combinations of private keys available, the PKG provides each joining node with a random and unused combination of private keys and the entire pool of public keys. Finally, the new nodes derive their identity from the obtained private keys. If all possible private key combinations are in use then the PKG must generate additional public-private key pairs to accommodate the new nodes. The new nodes obtain a new unique combination of private keys from the offline PKG and the extended pool of public keys. The node then derives its identity from the indexes of the obtained private keys. Once the new nodes go online, they broadcast the newly introduced public keys to every network node. This process is illustrated in Fig. 8(c). If the number of public keys has grown to a higher power of 2 then every node also updates their identity to contain sufficient bits. To prevent malicious nodes from broadcasting fake public keys, the offline PKG should sign the newly generated public keys.

He *et al.* [155], [156] mentioned that key revocation should be organized by the offline PKG since this authority also generates and maintains all the cryptographic keys. The offline PKG could resort to signing key revocation messages with every private key in the key pool, since only the offline PKG has access to these and every node has the public keys to verify the message. However, it is not mentioned which entity distributes these revocation messages since the PKG is considered to be offline.

3) EVALUATION FOR MOBILE SMALL CELLS

The security requirement is not met. He *et al.* [155] state that their scheme is secure against an identity impersonation attack, since a malicious node sending the identity of another node leads to an encrypted message which the malicious node is unable to decrypt. However, this scheme is vulnerable to an identity replacement attack. When a node A wishes the obtain the identity of a node B, but intermediate malicious node C replaces the identity of B for its own identity then the malicious node can decrypt any message sent by A intended for B. This attack is possible since the identity in this key management scheme is not derived from public knowledge, but works like a public key which requires verification for authenticity. Furthermore, the combinatorics approach which minimizes the memory requirement causes vulnerabilities against a mobile adversary. Suppose that node A (in possession of private keys sk_1 and sk_2) and node B (in possession of private keys sk_3 and sk_4) are compromised. Every node in possession of any other combination of two of these four private keys are now vulnerable to malicious attacks. Similarly, a malicious node launching a Sybil attack [87] could collect private keys in order to break the security of nodes having a combination of the obtained private keys.

The connectivity requirement is conditionally met. Under the assumption that identities can be securely exchanged and since every well-behaving network node is capable of obtaining its set of private keys, every arbitrary set of nodes is capable of establishing a secure channel, providing connectivity.

The sustainability requirement is not met. This is due to the lack of a proposed mechanism which deals with nodes leaving the network. If the key management allows the reuse of private key combinations and identities, then each node leaving the network has to contact the offline PKG such that it will be aware of recycling keying material. Then, the offline PKG could decide to send a revocation message to announce the inactivity of a formerly used identity. However, such a message only presents itself when another node joins the network. Furthermore, dynamic changes in network membership would cause the constant flood of messages throughout the network. It may therefore be more beneficial to not resort to the recycling of keying material. This means that every node will have a unique set of private keys and identity provided for the entire lifetime of the network. Due to the logarithmic growth of the memory requirement the overhead may still be acceptable, however key revocation messages will become unable to inform all network accessed nodes of compromised keys. It is necessary to create an efficient mechanism to deal with nodes leaving the network in order to satisfy the sustainability requirement.

The secure routing independence requirement is not met. This is due to fact that identities in this key management approach are created, like public keys are. Since these identities cannot be verified, they are vulnerable to replacement attacks by malicious intermediate nodes. The secure distribution of identities of multiple hops would require a secure routing protocol.

No issues have been identified related to the overhead, scalability and fairness requirement. Based on these evaluations, the authors believe that the pre-distribution-based key management approach will not be able to provide efficient and effective key management to support cryptographic protocols to secure a network of mobile small cells.

B. PARTIALLY DISTRIBUTED PKG-BASED KEY MANAGEMENT

The partially distributed PKG-based approach (PD-PKG) was introduced by Khalili *et al.* in [134]. This approach distributes the trust from an ordinary centralized PKG to a proper subset of network nodes and is therefore called partially distributed.

1) SYSTEM OVERVIEW

The general idea of the PD-PKG-based key management approach is distributing the trust from a single centralized trusted authority to a subset of nodes inside the network while keeping the overhead as low as possible. The distribution of trust is necessary since a MANET (for which it is designed) is unable to support a centralized PKG. Instead, the nodes forming the distributed PKG will provide network nodes with their private keys. Upon network initialization, n participating nodes create a master private key and the corresponding master public key in a distributed fashion. The master private key is created using the proposed t-out-of-n threshold cryptography scheme [159]. A node wishing to join the network uses its identity as its public key and contacts t of the initial nodes to construct its private key from the collected t partial private keys. An adversary wishing to break the security of the system must compromise t of the initial nodes during the lifetime of the network [118]. To prevent this attack from being successful, Khalili *et al.* [134] proposed to include proactive threshold cryptography. This means that shares are periodically refreshed such that it becomes impossible for an adversary to compromise t of the initial nodes within a share refreshing period. This provides robustness against active attackers.

2) SYSTEM DETAILS

This system consists of three main phases. The network initialization phase, the private key issuing phase, and the share updating phase. In the first phase, the network initialization phase, a set of n nodes collaboratively initialize the network by deciding on mutually acceptable security parameters. These security parameters include the threshold value t, particular parameters of underlying ID-based cryptographic schemes (e.g., key length), and a policy for key issuing. This initial set of nodes then creates the master private key and the corresponding master public key in a distributed fashion. The master private key is created using the proposed t-out-of-n threshold cryptography scheme [159] such that each of the n initial nodes obtains one share. This scheme also supports the verification of the shares. These nodes form the distributed PKG for an ID-based scheme, exchange their identities and start issuing private keys to each other. The master public key will be provided to all nodes joining the network. This process is illustrated in Fig. 9(a). Alternatively, [160]–[164] proposed to have an offline trusted authority select security parameters, create the master key-pair, and distribute shares of the master private key to n nodes in order to prevent any malicious nodes from establishing insecure key management during the network initialization phase.

In the second phase, the private key issuing phase, a node wishing to obtain its private key contacts at least t nodes which are a part of the PKG by moving into their transmission range. The node provides PKG-nodes with its identity and truthfully follows the key issuing policy to obtain partial private keys. This node can use t correct partial private keys to construct its personal private key. This process is illustrated in Fig. 9(b). To prevent adversaries from launching an impersonation attack, PKG-nodes should refuse to issue keys for a particular identity more than once. However, this will only be effective if $n < 2 \times k$ and it requires PKG-nodes to store the identities for which they already issued a partial private key. A multi-level hierarchical scheme was proposed in [165] in which a threshold of sibling nodes or parent nodes can issue a private key. In contacting the PKG-nodes, [160], [162] proposed to use the anonymous routing protocol MASK [166] to hide a nodes' identity by using pseudonyms. This prevents mobile adversaries from uncovering the PKG-nodes, therefore having to resort to compromising random nodes which significantly increasing the security of the system. However,

this may pose a problem when it comes to the secure routing interdependency problem.

For long-term networks, [161]–[164] introduced an additional public-private key updating phase. Private keys can be cryptanalyzed when the network lifetime is long enough, meaning that these keys also require to be updated periodically. To do this, the public key is created from a combination of the identity and a time stamp or key updating phase number which corresponds to a unique private key for every period between public-private key updating phases. In [165], [167], [168] a scheme is proposed in which network nodes determine which t out of n PKG-nodes are most likely to be well-behaving and should be contacted for key management services. This can significantly reduce the communication overhead when t trustworthy PKG-nodes are contacted periodically.

In the third phase, the share updating phase, the nodes forming the distributed PKG update their shares using proactive threshold cryptography [118] to prevent mobile adversaries from uncovering the master private key. Due to the exchange of identities and the issuance of private keys during the network initialization phase, these nodes have access to a secure channel to exchange subshares. This process is illustrated in Fig. 9(c).

Key revocation mechanisms were proposed in [161]–[163], [169] which use a Node Revocation List (NRL). When a node notices misbehavior from a neighboring node, it broadcasts an accusation to all the nodes inside the network. The accused node is now classified as ''suspect'' in every node's NRL. When a threshold amount of accusations is received within a certain time period, every node will reclassify the suspected node as ''convicted''. Any node will refuse communication or key management service to a convicted node and any accusations which came from a convicted node will be removed in each node's NRL.

To increase the scalability of this approach, [170] proposed the use of a clustered hierarchy in which the cluster-heads form the distributed PKG.

3) EVALUATION FOR MOBILE SMALL CELLS

The security requirement is conditionally met. As long as the initial n nodes initializing the network are well-behaving, trust is distributed throughout the network and the proper creation of private keys can be verified with the master public key. Proactive threshold cryptography provides robustness against mobile adversaries and verifiable threshold cryptography could be adopted from previously proposed schemes [93], [137] to allow easy detection of malicious behavior. Khalili *et al.* [134] mentioned that a node wishing to join the network could be vulnerable to a MITM attack. A malicious node could provide the joining node with a false master public key for which the malicious node has the corresponding master private key. Fortunately, this attack can be avoided when at least t PKG-nodes transmit the master public key along with the private key share. Furthermore, ID-PKC is known to suffer from the key escrow problem. This becomes problematic when an adversary is able to reconstruct the master private key. However, it is assumed that no adversary is able to collect at least t master private key shares within a share refreshing period.

The scalability requirement is not met. The scalability of the network is strongly related to the number of PKG-nodes acting as the distributed PKG since these PKG-nodes must provide all the network nodes with key management services. This means that a growth in the number of network nodes also increases the pressure on these PKG-nodes and subsequently reducing its battery life. It is reasonable to assume that the number of nodes in the mobile small cells fluctuate over time and could drastically increase in certain areas during sporting events, concerts and national celebrations. The limited amount of PKG-nodes could become incapable of providing key management services at this point. Khalili *et al.* [134] stated that network nodes are required to interact with the PKG-nodes only once in order to obtain their private key which reduces the impact, although this may not be enough to considered this scheme to be scalable from a connectivity perspective. Temporary on-demand auxiliary PKG-nodes could be adopted as a solution, as proposed in the PD-CA-based approaches [109], [135].

The sustainability requirement is met. Although it is reasonable to assume that the assigned PKG-nodes acting as a distributed PKG may leave the network at some point, resulting in an unavailable key management service followed by a disconnected network. A solution to this problem has been proposed in [136]. This key management scheme is also based on a partially distributed authority (although relying on certificateless PKC) and proposed a mechanism to replace a PKG-node in the event that one would leave the network. Due to the similarities of the key management structures, it is assumed that this mechanism can be easily adopted in the PD-PKG-based approach. This approach is therefore sustainable from a connectivity perspective. Furthermore, an increased network lifetime does not improve the abilities of adversaries to break security or worsen issues related to overhead.

The fairness requirement is not met due to the imbalance of overhead between network nodes. Even if PKG-nodes are replaced periodically in an attempt to fairly distribute the key management tasks and its associated overhead over time, user's mobile devices which are temporarily assigned as a PKG-node may still choose to act selfishly.

No issues have been identified related to the connectivity, overhead and secure routing independence requirement. Based on these evaluations, the authors believe that the PD-PKG-based key management approach will not be able to provide efficient and effective key management to support cryptographic protocols to secure a network of mobile small cells.

C. FULLY DISTRIBUTED PKG-BASED KEY MANAGEMENT

The fully distributed PKG-based approach (PD-PKG) was introduced by Deng *et al.* in [171], [172]. This approach distributes the trust from an ordinary centralized PKG evenly

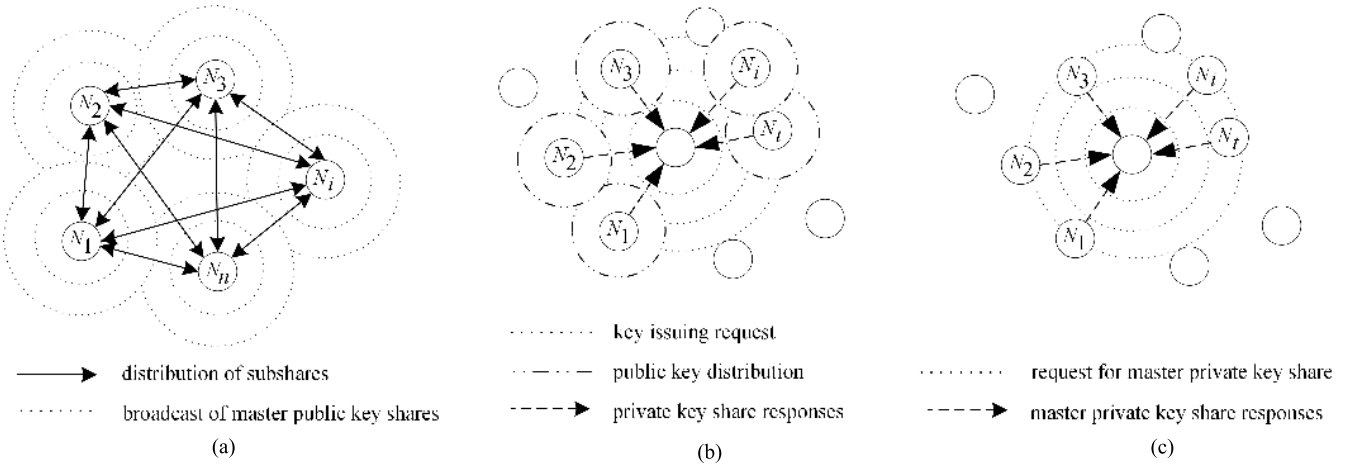

FIGURE 10. Illustration of the three main phases in the fully distributed private key generator-based approach. (a) Network initialization phase. (b) Public-private key issuing phase. (c) Master private key sharing phase.

among all the network nodes and is therefore called fully distributed.

1) SYSTEM OVERVIEW

Similar to the PD-PKG-based key management approach, the general idea is to distribute trust from a single centralized trusted authority to a set of network nodes due to MANETs (for which it is designed) being unable to support a centralized PKG. In this FD-PKG-based key management approach, trust is distributed among all the nodes. Upon network initialization, all the nodes wishing to participate in the network collaborate to generate a master private key using the proposed t-out-of-n threshold cryptography scheme [173] of which each node will hold a share. A master public key share is computed from these and then distributed to every network node such that everyone is able to construct the master public key. When a node wishes to join the network, it needs to broadcasts a request with identifying information to at least t neighboring nodes. These neighboring nodes decide on an expiration time, create the node's public key, and broadcasts this to all the nodes within the network. Then, each neighboring node uses their master private key share to create a share of the joining node's private key and a partial share for the joining node's master private key. These are then securely distributed to the joining node which can construct its private key and its master private key share upon obtaining t responses. This scheme is combined with verifiable threshold cryptography so the authenticity of the shares can be verified.

2) SYSTEM DETAILS

This system consists of three main phases. The network initialization phase, the public-private key issuing phase, and the master private key sharing phase. In the first phase, the network initialization phase, the n initial nodes collaboratively initialize the network by deciding on mutually acceptable security parameters and generating the master key pair. Deng *et al.* [171] and Deng and Agrawal [172] proposed using the threshold cryptography scheme as described in [173], since it removes the necessity of a trusted authority. In this scheme, each node contributes to the generation of the master private key by generating their own secret and then distribute subshares to the other nodes. Once the nodes receive all their subshares, they combine these to create their share of the master private key. It is assumed that the distribution of subshares take place offline since there is no mechanism in place yet to do this securely online. In [174], [175] it is proposed that nodes first distribute a temporary public-private key pair to enable the online distribution of shares. The master private key shares are then combined with a common parameter to create master public key shares. Each node broadcasts their master public key share such that every node can compute the master public key. This process is illustrated in Fig. 10(a). To remove any malicious nodes participating in the initialization process, [176], [177] proposed that nodes receiving faulty subshares broadcast this as a complaint. To avoid any malicious nodes participating in this process, [178] proposed to use an offline TA to initialize the system and distribute master private key shares. It is proposed by Deng *et al.* [171] and Deng and Agrawal [172] to adopt a verifiable threshold cryptography scheme to detect any invalid shares generated in the process, however there is no consensus which particular scheme should be used. Pedersen's verifiable threshold cryptography scheme [104] was proposed in [177], [179], Feldman's scheme [103] was proposed in [176] and Harn and Lin's scheme [180] was proposed in [175]. The following two phases are performed during the entire lifetime of the network.

The second phase, the public-private key issuing phase, is triggered when a node wishes to join the network or when a node's public key is about to expire. This node contacts at least t neighboring nodes to obtain its new public-private key pair. To reduce the communication overhead and delay,

[167] proposed to only contact the t most trustworthy nodes for key renewal. The most trustworthy nodes are selected based on local information from monitoring neighboring nodes. A joining node broadcasts a request in which it shares its identity *ID* and its MAC address, which are assumed to be unique and unchangeable. The neighboring nodes decide on the expiration time of the public key and create the public key $pk_{ID} = H(ID||MAC||Expire\_time)$ [141]. The MAC address and the expiration time are included in the public key to protect it against IP spoofing attacks and compromised private keys. However, the variable *Expire_time* may prevent a node's public key from being directly derived from publicly available information. It is therefore proposed that the neighboring nodes broadcast the node's public key (also called the network identifier *NID*) to everyone in the network. Instead, periodically updating public keys such that the public key is a concatenation of the identity and the period index number was proposed in [177]. However, this requires some form of synchronization and every node would send requests for a new private key at the same time. To reduce the communication overhead, [179] proposed to create the public key by concatenating the identity with a time stamp of issuing and that nodes only renew their public-private key pair when the node suspects that its key has been compromised. Unfortunately, this allows undetected compromised nodes to remain validated and cause further security issues [181]. After the public key is established, the neighboring nodes combine the node's public key with their share of the master private key to generate shares of the node's private key. These private key shares are distributed to the requesting node who combines these to create its private key. This process is illustrated in Fig. 10(b). A detailed key issuing protocol is described in [178] and claims to be resistant against replay attacks, MITM attacks and insider attacks without relying on a secure channel. However, this protocol relies on joining nodes to publish a hashed password along with their identity which need to be stored at network nodes and therefore eliminates the memory requirement advantage of ID-based schemes.

The third phase, the master private key sharing phase, follows the previous phase when a node joins the network. This node's identity has just been authenticated by its neighboring nodes and obtained its public-private key pair. These same neighboring nodes create a partial share of the master private key using their individual share. In order to protect the secrecy of the shares of these neighboring nodes, they may have to resort to some shuffling mechanism [138]. The neighboring nodes then distribute the partial shares to the joining node which combines them into its own master private key share. This process is illustrated in Fig. 10(c). To securely distribute the shares of the private key and the master private key, Deng *et al.* proposed that the joining node presents a self-generated temporary public key pk_{temp} which the neighboring service nodes use to encrypt the (master) private key shares before distributing these to the requesting node. A slightly alternative approach was presented in [182], which uses Feldman's verifiable threshold cryptography scheme [103] to create master private key shares which would also act as a node's private key. These shares are verifiable using the identity (or public key) of the node owning the share and can therefore act as the private key, simplifying the key management by combining the key issuing and the master private key sharing phases. This scheme is also based on the discrete logarithm problem instead of elliptic curves which improves computational efficiency.

It is proposed in [179] that the network lifetime should be divided into two distinct phases. An operational phase (containing the public-private key issuing phase and the master private key sharing phase for joining nodes) and a master private key share updating phase. During the master private key share updating phase a coalition of t nodes collaborate to generate a random share updating polynomial. Nodes within this coalition create subshares for each other and are distributed. These subshares allow the coalition to update their master private key share. However, no details are provided how nodes outside the coalition are supposed to update their master private key shares.

Deng *et al.* [171] and Deng and Agrawal [172] did not provide any details about key revocation. Revocation mechanisms are proposed in [169] and [181]. In these schemes a Node Revocation List (NRL), analogous to the CRL in certificate-based key management, is proposed. When a node notices misbehavior from a neighboring node, it broadcasts an accusation to all the nodes inside the network. The accused node is now classified as a ''suspect'' in every node's NRL. When a threshold amount of accusations is received within a certain time period, every node will reclassify the suspected node as ''revoked''. Any node will refuse communication or key management service to a revoked node and any accusations which came from a revoked node will be removed in each node's NRL.

3) EVALUATION FOR MOBILE SMALL CELLS

The security requirement is conditionally met. As long as the initial n nodes initializing the network are well-behaving, trust is distributed throughout the network such that the proper creation of private keys can be verified with the master public key. Proactive threshold cryptography could be adopted from previously proposed schemes [93], [134], [137]–[140] to provide robustness against mobile adversaries [118] while verifiable threshold cryptography allows the easy detection of malicious behavior. However, a node wishing to join the network could be vulnerable to a MITM attack [134]. This malicious node could provide the joining node with a false master public key for which the malicious node has the corresponding master private key. Fortunately, this attack can be avoided when at least t nodes transmit the master public key along with the private key share since a mobile adversary is assumed to be incapable of simultaneously controlling t network nodes. Furthermore, the FD-PKG-based approach is vulnerable to a Sybil attack [87]. In the Sybil attack a malicious user takes on multiple (in this case at least t) identities, thereby

representing multiple nodes of which each has the ability to obtain a share derived from the master private key. For example, the malicious user could purchase t mobile devices and register these with different network providers in order to successfully register t devices and obtain t shares. This would allow the malicious user to recreate the entire master private key and break security within the system. This attack can be prevented by implementing policies, such as limiting the distribution of shares to one share per identity (which can be maintained through identity authentication) instead of one share per mobile device/SIM. Moreover, ID-PKC is known to suffer from the key escrow problem. This becomes problematic when an adversary is able to reconstruct the master private key, since this enables the adversary to compute a node's private key and therefore break the security of the entire system. CB-PKC and CL-PKC do not suffer from the key escrow problem, meaning that backward secrecy is still protected against. However, it is assumed that no adversary is able to collect at least t master private key shares within a share refreshing period.

The scalability requirement is met. Although the proposed master key-pair generation process does not scale to large groups, this is not necessary during the network initialization phase. A large group during network initialization even increases the chances that a malicious node is involved in the initialization process. Additionally, scalable mechanism presented in other distributed authority-based schemes could be adopted [137]–[140]. This provides scalability from an overhead perspective. Furthermore, nodes are able to join and leave the network at any time without posing issues related to security or connectivity.

The sustainability requirement is conditionally met even though the initial proposal by Deng *et al.* [171] and Deng and Agrawal [172] does not include proactive threshold cryptography to prevent a mobile adversary from collecting at least t shares of the master private key over time. Mechanisms introduced in the other distributed authority-based approaches which include proactive threshold cryptography [93], [134], [137]–[140], [183] can be adopted to provide resiliency against mobile adversaries for this key management approach. This provides sustainability in this key management approach from a security perspective. Furthermore, an increased network lifetime does not worsen issues related to connectivity or overhead.

No issues have been identified related to the connectivity, overhead, fairness and secure routing independence requirement. Based on these evaluations, the authors believe that the FD-PKG-based key management approach has potential to provide efficient and effective key management to support cryptographic protocols to secure a network of mobile small cells.

VI. CERTIFICATELESS KEY MANAGEMENT SCHEMES

Certificateless public key cryptography (CL-PKC) was introduced by Al-Riyami and Paterson *et al.* [41] in 2003. It was introduced as an alternative to CB-PKC, which suffers from expensive certificate management, and ID-PKC, which suffers from the key escrow problem. It could be described as a hybrid between CB-PKC and ID-PKC attempting to only keep the benefits of each scheme. Therefore, a network node uses two key pairs to establish secure communication. It first creates a mathematically linked key pair, similar to a key pair used in CB-PKC, while also using its identity as a second public key and its corresponding private key obtained from the TTP. This TTP is called a Key Generation Center (KGC). A network node wishing to communicate with the key pair owner would request the (certificateless) public key and uses this key along with the owner's identity to establish secure communication. The (certificateless) public key does not require authentication from a TTP since an adversary is unable to benefit from a key replacement attack due to the adversary not having access to the identity-based private key. At the same time, the mathematically linked private key is only known to the network node which prevents the key escrow problem. The design by Al-Riyami and Paterson [41] limits key management algorithms to ECC [42], therefore Baek *et al.* [184] and Lai and Kou [185] proposed their own CL-PKC designs which does not have this limitation.

This chapter discusses two key management approaches relying on CL-PKC. The partially distributed KGC-based approach and the fully distributed KGC-based approach.

A. PARTIALLY DISTRIBUTED KGC-BASED KEY MANAGEMENT

The partially distributed KGC-based approach (PD-KGC) was introduced by Zhang *et al.* in [136]. This approach distributes the trust from an ordinary centralized KGC to a proper subset of network nodes and is therefore called partially distributed.

1) SYSTEM OVERVIEW

The general idea of the PD-KGC-based key management approach is distributing the trust from a single centralized trusted authority to a proper subset of nodes inside the network. The network is initialized by a KGC and n nodes. The KGC first generates a master public key and a master private key after which it authenticates the n nodes and provides them with an ID-based private key such that every node is able to create their public-private key pair. During the authentication process, the KGC selects k nodes which it deems to be trustworthy and provides these nodes with shares of the master private key created from a t-out-of-k ($t \leq k \leq n$) threshold cryptography scheme [186]. These distributed KGC-nodes are able to provide key management services. The offline KGC leaves the network and the network initialization process is complete. When a new node wishes to join the network, it has to contact at least a threshold t number of KGC-nodes to obtain its ID-based private key from which it can construct its public-private key pair. When a KGC-node leaves the network, a set of at least t active KGC-nodes select a random network node to replace the leaving KGC-node. The KGC-nodes provide the replacement node with its own

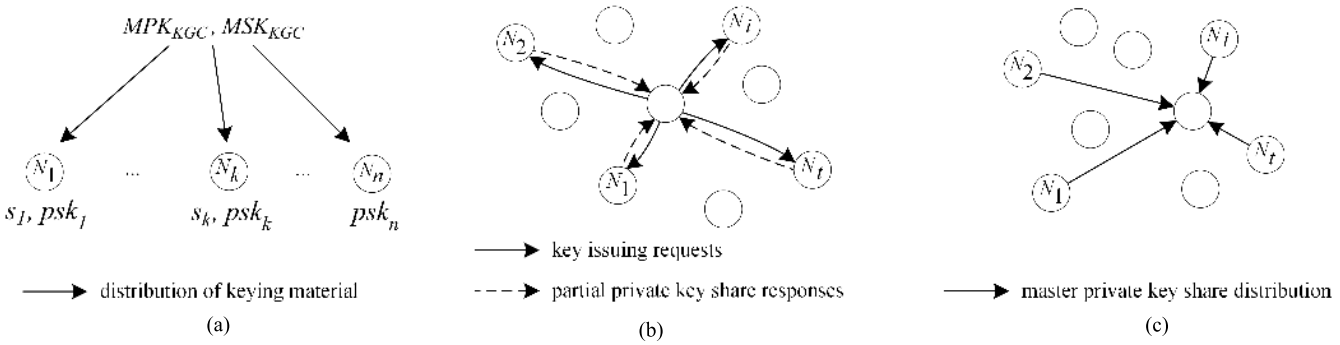

FIGURE 11. Illustration of the three main phases in the partially distributed key generation center-based approach. (a) Network initialization phase. (b) Private key issuing phase. (c) KGC node replacement phase.

master private key share, such that there are k KGC-nodes active within the network during the entire network lifetime. Zhang *et al.* [136] provides detailed algorithms for the various key management services and they are based on the work by Al-Riyami and Paterson [41].

2) SYSTEM DETAILS

This system consists of three main phases. The network initialization phase, the private key issuing phase, and the distributed KGC-node replacement phase. In the first phase, the network initialization phase, there is an offline KGC and n nodes which will initialize the network. Out of these n nodes, k nodes are selected to form the distributed KGC. First, the offline KGC executes a setup algorithm which generates the master public key and the master private key. Then, the offline KGC uses the master private key to create an ID-based private key for each node and uses a t-out-of-k threshold cryptography scheme [186] to divide the master private key into k shares. The offline KGC distributes these shares among k of the n nodes and the ID-based private keys among all n nodes. This process is illustrated in Fig. 11(a). Finally, the KGC publishes the master public key and goes offline. Each node can now create their own public-private key pair. The following two phases are performed during the entire lifetime of the network.

The second phase, the private key issuing phase, is triggered when a new node wishes to join the network. This node contacts t KGC-nodes requesting shares of its ID-based private key. Each contacted KGC-node authenticates the joining node, creates a share of the node's ID-based private key and transmits this to that node. This process is illustrated in Fig. 11(b). Once the joining node obtains t shares of its ID-based private key, it combines them to create its ID-based private key. Detailed algorithms can be found in [136] and are based on Al-Riyami *et al.*'s work [41]. An adversary could still replace un-authenticated public keys to perform a denial-of-decryption attack. This attack wastes network resources and [187], [188] proposed to bind the public key of a node to its identity and their ID-based private key to counter this. Furthermore, shares of ID-based private keys are claimed to be distributable over public channels since eavesdroppers would not learn anything from the node's combined private key [187], [188]. However, security can be broken when an eavesdropper learns about the ID-based private key and successfully performs a key replacement attack on the same node's public key.

The third phase, the distributed KGC-node replacement phase, is triggered when a KGC-node leaves the network. When a KGC-node leaves the network, a random non-KGC-node is selected to take its place. Other KGC-nodes create a partial master private key share using their own shares. These partial shares are then distributed to the selected non-KGC-node which combines them into its own master private key share. This process is illustrated in Fig. 11(c). This phase ensures that there are always k online KGC-nodes available to provide key management services. It is not specified how a leaving KGC-node is detected or how the KGC-nodes select a non-KGC-node to replace the leaving KGC-node.

Key revocation mechanisms are proposed in [189], [190]. When a node detects malicious behavior it transmits an accusation message to the KGC-nodes. A certain threshold of accusations against the accused node is required in [189] before KGC-nodes start to cooperate to generate a revocation message and flood the network with it. Each node verifies the revocation message and records the identity of the revoked node in its memory.

No scheme within this approach mentions a master private key share updating mechanism to prevent a mobile adversary [118] from collecting t master private key shares and reconstructing the master private key.

Many of the mentioned schemes rely on ECC which suffers from computationally expensive pairing operations. To reduce the amount of pairing operations [191]–[194] proposed schemes which combine ECC with RSA.

3) EVALUATION FOR MOBILE SMALL CELLS

The security requirement is met since trust is distributed throughout the network and the proper creation of ID-based private keys can be verified with the master public key.

Proactive threshold cryptography could be adopted from previously proposed schemes [93], [134], [137]–[140] to provide robustness against mobile adversaries while verifiable threshold cryptography could be adopted from previously proposed schemes [93], [137] to allow easy detection of malicious behavior. However, a node wishing to join the network could be vulnerable to a MITM attack [134]. A malicious node could provide the joining node with a false master public key for which the malicious node has the corresponding master private key. Fortunately, this attack can be avoided when t KGC-nodes transmit the master public key along with the ID-based private key share.

The scalability requirement is not met. The scalability of the network is strongly related to the number of KGC-nodes acting as the distributed KGC since these KGC-nodes must provide all the network nodes with key management services. A growth in the number of network nodes also increases the pressure on these KGC-nodes and subsequently reducing its battery life. It is reasonable to assume that the number of nodes in the mobile small cells fluctuate over time and could drastically increase in certain areas during sporting events, concerts and national celebrations. The limited amount of KGC-nodes could become incapable of providing key management services at this point. This scheme is therefore not considered scalable from a connectivity perspective. Temporary on-demand auxiliary KGC-nodes could be adopted as a solution, as proposed in the PD-CA-based approach [109], [135].

The sustainability requirement is conditionally met even though the initial proposal by Zhang *et al.* [136] does not include proactive threshold cryptography. Mechanisms introduced in the other distributed authority-based approaches which include proactive threshold cryptography [93], [134], [137]–[140], [183] can be adopted to provide resiliency against mobile adversaries. This provides sustainability in this key management approach from a security perspective. Furthermore, an increased network lifetime does not worsen issues related to connectivity or overhead.

The fairness requirement is not met due to the imbalance of overhead between network nodes. Even if PKG-nodes are replaced periodically in an attempt to fairly distributed the key management tasks and its associated overhead over time, user's mobile devices which are temporarily assigned as a PKG-node may still choose to act selfishly.

No issues have been identified related to the connectivity, overhead and secure routing independence requirement. Based on these evaluations, the authors believe that the PD-KGC-based key management approach will not be able to provide efficient and effective key management to support cryptographic protocols to secure a network of mobile small cells.

B. FULLY DISTRIBUTED KGC-BASED KEY MANAGEMENT

The fully distributed PKG-based approach (FD-PKG) was introduced by Li *et al.* in [183]. This approach distributes the trust from an ordinary centralized PKG evenly among all the network nodes and is therefore called fully distributed.

1) SYSTEM OVERVIEW

The general idea of the FD-KGC-based key management approach is distributing the trust from a single centralized trusted authority to all the nodes inside the network. The network is initialized by n nodes which collectively generate the master public key and master private key. At the end of network initialization, each node has a share of the master private key which they can use to create ID-based private keys to authenticated nodes and provide new master private key shares to nodes joining the network. To prevent any malicious nodes from creating false keying information, verifiable threshold cryptography [103], [195], [196] is proposed to authenticate keying information. To prevent mobile adversaries [118] from collecting enough master private key shares and compromise the system, proactive threshold cryptography is proposed [98].

2) SYSTEM DETAILS

This system consists of three main phases. The network initialization phase, the node joining phase, and the share updating phase. In the first phase, the network initialization phase, n nodes initialize the network following Pedersen's threshold cryptography scheme without a trusted authority [195]. In this process, every node create its own secret, the corresponding witness values and a subshare for every other node. The witness values are broadcasted and the individual subshares are securely exchanged. This process is illustrated in Fig. 12(a). The nodes use the witness values to verify the correctness of the obtained subshares and once a node obtains enough subshares, it combines them into its master private key share. Li *et al.* [183] does not discuss how each node obtains the master public key. A solution to this was proposed in [197], stating that each node creates their master public key share from their master private key share and broadcasts this. Each node combines t master public key shares into the master public key. In [136], [198], [199] the presence of a TTP is assumed which generates the master key pair and distributes shares of the master private key among the initial network nodes to initialize the network.

After each node obtains a share of the master private key, they create a mathematically linked public-private key pair and publishes the public key. A node then contacts its neighboring nodes and requests shares for its ID-based private key. Once this node obtains t valid shares it combines them (and its mathematically linked private key) into its combined private key. The following two phases are performed during the entire lifetime of the network.

The second phase, the node joining phase, is triggered when a new node wishes to join the network. This node creates a mathematically linked public-private key pair and publishes the public key. Then, the node wishing to join the network presents its identity, public key, and some other required physical proof to at least t network nodes and

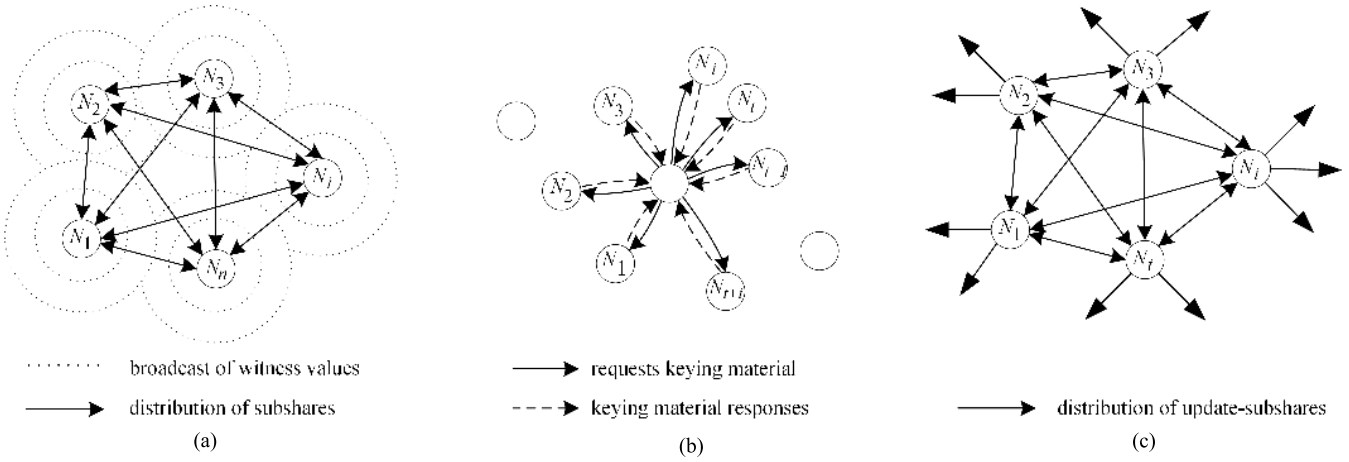

FIGURE 12. Illustration of the three main phases in the fully distributed key generation center-based approach. (a) Network initialization phase. (b) Node joining phase. (c) Share updating phase.

requests shares of its ID-based private key and partial shares of its master private key. Each contacted node needs to verify the identity of the requestor prior to sending any keying information. If the identity verification succeeds, the contacted node generates a share of the ID-based private key, generates a partial share of the master private key, encrypts these using the requestor's public key, and transmits the encrypted keying information along with the master public key. This process is illustrated in Fig. 12(b). In [197] the existence of a trusted authority is assumed which decides whether a node may join the network. This effectively removes the identity verification process by the contacted KGC-nodes.

Once the joining node receives at least t responses, it decrypts and verifies the keying information. The t correct shares of the ID-based private keys will be combined to create the ID-based private key which in turn is combined with the node's mathematically linked private key to create its full private key. The partial shares of the master private key are combined to create its own master private key share. The new node is now capable of decrypting any received messages which were encrypted with its public key and identity, and it can provide key management service to other joining nodes. In [198], [199] it is argued that the initially obtained keys should act as the personal master key only to be used in a key derivation function to create keys which will be used for cryptographic applications.

An interesting idea is discussed in [197]. It proposes that the master key pair should continue to consist of contributions made by each node within the network. This means that a node which joins the network creates its own secret, generates subshares for every node already inside the network and distributes these securely to them. Each node then updates their master private key share and generates a subshare for the joining node which it combines into its own master private key share. Master public key shares are also shared and updated. Similarly, when a node leaves the network, the node announces its departure and the remaining network nodes remove its contribution from the master private key share and master public key. This scheme updates keys upon membership changes of the network. However, this comes with additional communication and memory storage overhead of which the expense increases exponentially with the size of the network.

The third phase, the share updating phase, is proposed to protect the system against mobile adversaries. Such an adversary compromises nodes one at a time in order to collect t master private key shares such that it can reconstruct the master private key and compromise the system. It is assumed that a mobile adversary can only collect $t-1$ shares between any consecutive share updating phase. Therefore, the share refreshing phase is initiated by t nodes and uses verifiable threshold cryptography to detect any malicious behavior. These t nodes each select a random update polynomial and securely send an update subshare for every node within the network. This process is illustrated in Fig. 12(c). When a node receives these t update subshares, it combines these into a full update subshare and then with the original master private key share to create a new master private key share. This master private key share is independent of the previous share which means that a mobile adversary is unable to use formerly collected master private key shares and uncover the master private key.

A key revocation mechanism is proposed in [190] and is triggered once malicious behavior at a network node is detected. A coalition of t nodes generate partial revocation messages and the assigned coalition leader combines these partial revocations. The coalition leader then distributes the revocation message to all the nodes within the network. Each node verifies the validity of the revocation message and, if correct, stores the identity of the malicious node to deny any future communication with it.

To establish secure communication [183], [190] proposed an interactive key agreement scheme while [136], [197] proposed an encryption and decryption scheme. In each of these

schemes the public key of the other node is requested and verified as a valid public key. However, the public keys do not seem to be bound to the node's identity and these schemes may therefore be vulnerable to a key replacement attack [188] which disrupts communication and wastes network resources.

3) EVALUATION FOR MOBILE SMALL CELLS

The security requirement is met as long as the initial n nodes initializing the network are well-behaving. Verifiable threshold cryptography allows the detection of malicious behavior and proactive threshold cryptography provides robustness against mobile adversaries. However, a node wishing to join the network could be vulnerable to a MITM attack [134]. A malicious node could provide the joining node with a false master public key for which the malicious node has the corresponding master private key. Fortunately, this attack can be avoided when t nodes transmit the master public key along with the private key share. Furthermore, the FD-KGC-based approach is vulnerable to a Sybil attack [87]. In the Sybil attack, a malicious user takes on multiple identities, thereby representing multiple nodes, to gather enough master public key shares to break security. For example, this malicious user could purchase t mobile devices and register these with different network providers in order to successfully register t devices and obtain t shares. This would allow the malicious user to recreate the entire master private key. This attack can be prevented by implementing policies, such as limiting the distribution of shares to one share per identity (which can be maintained through identity authentication) instead of one share per mobile device/SIM.

The scalability requirement is met. Although the proposed master key-pair generation process does not scale to large groups, this is not necessary during the network initialization phase. A large group during network initialization even increases the chances that a malicious node is involved in the process. Additionally, the proposed share updating mechanism requires a flood of t subshares throughout the entire network, whereas the proposal in [137]–[140] only floods the network with an update polynomial. This mechanism could potentially be adopted to minimize the communication overhead. Then, this scheme provides scalability from an overhead perspective. Furthermore, nodes are able to join and leave the network at any time without posing issues related to security or connectivity.

No issues have been identified related to the connectivity, overhead, sustainability, fairness and secure routing independence requirement. Based on these evaluations, the authors believe that the FD-KGC-based key management approach has potential to provide efficient and effective key management to support cryptographic protocols to secure a network of mobile small cells.

VII. SYMMETRIC KEY MANAGEMENT SCHEMES

In symmetric key cryptography (SKC), a set of network nodes wishing to securely communicate with each other are provided with a shared key which they use for both encryption and decryption purposes. The secrecy of this shared key, being only known by the involved network nodes, provides security in this family of cryptographic key management. Two main advantages of symmetric keys over asymmetric keys (used in PKC) is that each key does not require as many bits while providing similar amounts of security and that cryptographic primitives, such as encryption and decryption schemes like AES [200], are computationally more efficient and therefore also more energy efficient. However, this generally comes at the expense of flexibility in areas such as scalability and dynamic membership which are important characteristics of ad hoc networks. The advantages of symmetric key management are particularly helpful to resource restricted devices such as wireless sensors such that many key management proposals for dynamic sensor networks (DSNs) attempt to mitigate the disadvantages of having to resort to symmetric key management. These resource restrictions do not apply to the user equipments considered in our scenario architecture, MANETs and ad hoc D2D networks and can therefore enjoy the flexibilities offered by PKC. Yet, some symmetric key management schemes have been proposed for MANETs and ad hoc D2D networks while attempting to mitigate some of the disadvantages. There are three main classes of organizing the symmetric key management such that network nodes can establish their shared keys in an authenticated manner, namely key pre-distribution, key distribution and key agreement.

A. KEY PRE-DISTRIBUTION-BASED KEY MANAGEMENT

This class of symmetric key management schemes, independently introduced by Blom [201] and Matsumoto and Imai [202], is organized by a TTP named the Key Distribution Center (KDC). This KDC provides each network node with long-lived symmetric keys during the network initialization phase. These keys are generally used to create pairwise keys to secure P2P communication. The exact pre-distribution of keys depends on the security requirements of the network. For a network which requires strong security, the KDC would distribute a pairwise key for every pair of network nodes. Every node in a network of n nodes will therefore obtain $n-1$ pairwise keys which causes a high memory requirement. However, any pair of nodes which has not been compromised by an adversary is guaranteed to remain secure. A network which does not require such strong security standards can use alternative key pre-distribution schemes in order to reduce the memory requirement. These schemes provide security against eavesdroppers as long as a certain threshold of network nodes are not colluding and have not been compromised [203].

Once every node is provided with keying material, network initialization is complete and every pair of nodes can use their symmetric keys to establish a secure communications channel between each other. During this time, the KDC is considered to be offline. This is the only class of symmetric key management that is resilient against dynamic

topological changes inside the network [204], [205] while the offline KDC prevents adversaries from having to compromise only a single target to compromise the security of the entire network. However, a problem occurs when nodes wish to join the network during network deployment. These nodes are unable to establish pairwise keys with nodes which are already part of the network. Suppose that the new nodes are able to obtain keying material in an offline fashion from the KDC prior to joining the network, the offline KDC is still unable to provide the online nodes with keying material such that they can authenticate the joining nodes and establish a secure communications channel with them. Thus, the class of key pre-distribution-based key management is unable to support certain membership changes in dynamic ad hoc networks [36], [37].

Two works [204], [205] proposing a key management scheme for DSNs based their schemes on key pre-distribution and claim that key pre-distribution is the only practical option out of the three classes of symmetric key management. Chan [206], [207] used this advice when he proposed a key management scheme for a MANET in which he attempted to solve the disadvantage of membership changes inherent in key pre-distribution schemes. He introduced the use of a large public set of private keys of which nodes would select a random subset for personal use. Chan provided a shared-key discovery protocol in which network nodes interactively can discover which private keys they have in common while preventing one another from revealing the private keys that they do not have in common. These shared keys would then be used to secure communication between these nodes. Chan claimed that his scheme has a high probability that users share at least one private key with each other while providing resiliency against colluding (or compromised) network nodes attempting to uncover shared private keys between other nodes. Goratti *et al.* [208] proposed a similar approach to secure communications for an ad hoc D2D network. Unfortunately, Wu and Wei [209] pointed out a flaw which nullifies Chan's claim and shows that either a high probability of a shared private key can be guaranteed or resiliency against colluding network nodes but not both at the same time making the approach impractical. No other symmetric key management scheme based on key pre-distribution has been found which would make a suitable candidate to secure a network of mobile small cells.

B. KEY DISTRIBUTION-BASED KEY MANAGEMENT

This class of symmetric key management schemes is also organized by a KDC. Each node wishing to participate in the network contacts the KDC in an offline and secure fashion to obtain a shared private key. This shared private key enables each node to establish a secure channel with the KDC during network deployment. When a network node wishes to securely communicate with another network node (or a group of network nodes) it contacts the online KDC and follows an interactive protocol which results in each of these network nodes obtaining a temporary common key. The class of key distribution schemes therefore establishes keys on demand and it supports both P2P key management schemes as well as group key management schemes.

Key distribution schemes have the advantage that every network node is only required to store a single long-lived symmetric key which they share with the KDC and therefore does not suffer from a large memory requirement as might be the case in a key pre-distribution scheme. However, key distribution schemes have several issues in a dynamic ad hoc environment. Several key distribution-based schemes [210]–[214] proposed for an ad hoc network rely on the online centralized KDC to organize the key management which is not only difficult to support but it also poses a security risk. DoS attacks could make the key management service unavailable and a compromise of the KDC would compromise all the keys that it issues. An ad hoc network could overcome this single-point-of-attack by selecting a group of online network nodes to perform the task of the KDC as is proposed in [215] but in order to establish trust this scheme relies on an underlying public key management scheme. Even if a centralized or a decentralized KDC could be supported and secured against malicious attacks, it may still not be able to set up secure communication between nodes due to communication range limitations, network partition and link breakages caused by node movement or the unknown network topology prior to network deployment. No symmetric key management scheme based on key distribution has been found which does not rely on a centralized KDC or an underlying public key management scheme to make a suitable candidate to secure a network of mobile small cells.

C. KEY AGREEMENT-BASED KEY MANAGEMENT

In the class of key agreement schemes, multiple network nodes contact each other to establish a shared symmetric key. These nodes follow an interactive protocol in which each node contributes some secret input in the creation of this key. This key can then be used to secure communication. The major advantage of this scheme is that the interactive protocol is fully distributed, self-organized and it does not rely on a TTP. However, this class of schemes also comes with drawbacks.

The interactive protocol is not robust against the topological changes and link breakages which occur in networks with a dynamic topology. This is especially troublesome for the establishment of a shared group key since this requires more time and more message exchanges to complete the protocol. Furthermore, key agreement schemes would also require support of a routing infrastructure since it is likely that two nodes wishing to communicate are not within each other's transmission range and therefore have to rely on intermediate nodes forwarding messages. As already discussed, secure routing is not available at this stage which means that these protocols are vulnerable to MITM attacks. The only way to prevent MITM attacks is by combining the key agreement scheme with a mutual authentication scheme. These are also called authenticated key agreement

TABLE 3. Evaluation and comparison table of described key management approaches.

Key Management approach	Security	Connectivity	Overhead	Scalability	Sustainability	Fairness	Secure Routing Ind.
Certificate Chaining-based [53], [54]			✓	✓	✓	✓	
Mobility-based [85], [86]	✓		✓	✓	✓	✓	✓
Self-Certification-based [91]		✓			✓	✓	✓
PD-CA-based [93]	✓	✓			✓		✓
FD-CA-based [137]–[140]	✓	✓		✓	✓	✓	✓
Pre-Distribution-based [155], [156]		✓	✓	✓		✓	
PD-PKG-based [134]	✓	✓	✓		✓		✓
FD-PKG-based [171], [172]	✓	✓	✓	✓	✓	✓	✓
PD-KGC-based [136]	✓	✓	✓		✓		✓
FD-KGC-based [183]	✓	✓	✓	✓	✓	✓	✓

schemes (AKAS). Shen *et al.* [216] proposed to include a short visual or verbal message for the purpose of mutual authentication. Unfortunately, identity and location privacy issues arise from this ordinary form of mutual authentication. Anonymous mutual authentication is necessary to tackle these issues. However, anonymous mutual authentication relies on a pre-established secret between the network nodes. This pre-established secret is provided by an underlying key pre-distribution scheme [217], [218], key distribution scheme (also known as a trusted server scheme) or public key cryptography-based scheme (also known as a self-enforcing scheme) [219]–[223]. Due to this reliance on an underlying key management scheme, key agreement schemes are not explored further in this article.

VIII. EVALUATION AND COMPARISON OF KEY MANAGEMENT APPROACHES

Based upon an extensive evaluation, we summarized in Table 3 the key management approaches and their abilities to satisfy each proposed requirement. It is clear that many key management approaches fail to satisfy every proposed requirement to secure a network of mobile small cells. However, some failed requirements could potentially be resolved by proposed solutions. This chapter compares the evaluation of each key management approach and highlights the main drawbacks and its ability to overcome these in order to be considered as a candidate to secure the mobile small cells network.

The certificate chaining-based approach [53], [54] is considered insecure due to its reliance of transitive trust. We demand a high level of security which this approach is unable to satisfy. Furthermore, if transitive trust is considered secure for an alternative ad hoc network use case, the reliance on secure routing to exchange certificate repositories still poses a problem.

The mobility-based approach [85], [86] is only considered conditionally secure. Again, this is due to its reliance on transitive trust. By eliminating mechanisms to exchange keying material which rely on transitive trust, keying material can only be obtained through mobility and close-proximity authentication. This not only leaves us with a highly disconnected network, it also causes issues related to overhead and scalability. This approach has the potential to satisfy six individual requirements, however it is unable to satisfy all of these at the same time. Furthermore, it is not realistic to have device owners exchange keying material based on mobility when they could simply rely on existing network infrastructure to connect them.

The self-certification-based approach [91] generates a tremendous amount of communication overhead in a dense and highly dynamic network due to its neighborhood monitoring process. This provides security and connectivity but cannot simply be adjusted without breaking the entire key management. This is the major drawback which makes this approach unlikely to efficiently secure a network of mobile small cells.

The pre-distribution-based approach [155], [156] is outright insecure due to the exchange of identities, essentially public keys, which have no means of verification. This could be resolved by secure routing, however this is not possible at this stage. If a solution to this problem can be found, then the pre-distribution-based approach still requires an efficient mechanism which deals with nodes leaving the network.

All of the partially distributed TTP-based approaches (PD-CA [93], PD-PKG [134], PD-KGC [136]) suffer from the asymmetric relationship and workload of the network nodes. This asymmetry promotes free-riding and could cripple the key management and its provided security of the entire network. Stimulating cooperation mechanisms will therefore be increasingly difficult to develop.

Almost all of the fully distributed TTP-based approaches (FD-CA [137]–[140], FD-PKG [171], [172], FD-KGC [136], [183]) satisfy every requirement and has the potential to satisfy these at the same time. Security challenges can be overcome while these approaches provide connectivity, scalability, sustainability, fairness, and routing independence. However, the FD-CA-based approach suffers from a comparatively large communication overhead due to the certificate

management and distribution. These approaches are based on a MANET architecture. The adoption of this approach for mobile small cells provides opportunities when it comes to the key management and routing since assistance from the network infrastructure is available. Overall, the fully distributed TTP is considered an approach worth pursuing to secure a network of mobile small cells.

IX. KEY MANAGEMENT FOR NETWORK CODING-ENABLED NETWORKS

A network coding-enabled network allows the encoding of data at routers and the decoding at the receiver. Network coding, introduced by Ahlswede *et al.* in [25], provides significant benefits to networks in terms of bandwidth, energy consumption, delay and robustness. Despite these advantages, networks utilizing the network coding technology are vulnerable to the so-called pollution attack. In this attack, a malicious user controls a router and mutates data by polluting them. Network coding causes this pollution to spread downstream by encoding correct data with polluted data. This leads to the inability to properly decode and retrieve the information at the receiver. Pollution attacks therefore waste many costly network resources. Data integrity schemes are required to prevent any polluted data from being transmitted any further through the network. However, this is only possible if the source node provides every intermediate node with a piece of verifiable information and therefore must share a cryptography key with them. The research community proposed various integrity schemes [224]–[232], but they all rely on an efficient key management scheme. Also, in order to utilize network coding there must exist at least two intertwined multihop paths between the source node and the destination node. The most important requirement of a key management scheme for network coding-enabled networks is therefore connectivity.

X. OPEN RESEARCH CHALLENGES

This survey has identified two open research challenges related to designing a suitable key management scheme to secure a network of mobile small cells.

Key management schemes relying on a partially distributed TTP require a rigorous procedure for selecting the most suitable network nodes to act as the distributed TTP. The selected nodes could be random, based on physical security and computational ability [105]–[111], trustworthiness [112], [113], restricted mobility, maximum clique [114], [115] or any other parameter. Furthermore, nodes acting as the distributed TTP require a replacement procedure if any decide to leave the network. The aim of the researchers should be to prevent the selected nodes from acting selfishly due to the overhead burden, while the key management services are provided with limited delay. The many considerations in the selection procedure keeps this process an open research area.

Due to the lack of network infrastructure in MANETs, key management schemes designed for this type of network relies on physical contact to instantiate trust and distribute keys. This form of authentication to secure communication is not realistic in a network of mobile small cells, since network users could utilize the existing network infrastructure. Network nodes wishing to authenticate each other online therefore seem to require assistance from the network infrastructure. Authentication schemes to secure D2D communications have been proposed [23], [214], but it assumes the network infrastructure to be secure against compromise. An authentication scheme between these parties which prevents distribution of sensitive and private data over insecure channels is an open research area.

XI. CONCLUSIONS AND FUTURE DIRECTIONS

Covering the urban landscape with mobile small cells, as proposed by the EU funded H2020-MSCA project "SECRET", optimizes network services such as data rates, energy efficiency, latency, and interference in a cost-effective fashion. In this network architecture, we do not assume the existence of an online centralized TTP which is resilient against compromise. We believe that the network infrastructure is unable to act as the trust anchor since network infrastructure could potentially be physically broken into such that transmissions of cryptographic keying material can be falsified or that network infrastructure can become unavailable to perform key management services due to denial-of-service attacks. Therefore, a key management scheme which provides secure communication between mobile devices within a network of mobile small cells is required to decentralize trust and must therefore be self-organized during network deployment.

In this article, we have studied ten key management schemes which attempt to distribute trust. All of these are based on PKC, of which five key management approaches rely on CB-PKC, three key management approaches rely on ID-PKC, and two key management approaches rely on CL-PKC. No key management scheme based on symmetric key cryptography has been found which successfully removes the necessity of an online centralized TTP. This article explores each studied key management approach extensively by including many works proposing improvements, adjustments or extensions of the original proposal. This creates a deep understanding of each key management approach and their potential when it comes to its adoptability into the proposed scenario architecture.

Self-organized key management schemes must satisfy seven proposed requirements in order to become eligible for adoptability. These requirements cover security, connectivity, overhead, scalability, sustainability, fairness and secure routing independence. Each key management approach has been evaluated for these seven requirements and we have found that only the FD-PKG-based key management approach and the FD-KGC-based key management approach have the potential to satisfy all of them. The other key management approaches were evaluated to be unfitting to properly secure the network of mobile small cells due to drawbacks to which no solution may exist. Therefore, as a future work we plan to design a novel key management scheme utilizing ideas

proposed in the FD-PKG-based and the FD-KGC-based key management approach.

REFERENCES

[1] E. Hossain and M. Hasan, "5G cellular: Key enabling technologies and research challenges," *IEEE Instrum. Meas. Mag.*, vol. 18, no. 3, pp. 11–21, Jun. 2015.
[2] Ericsson, "More than 50 Billion connected devices (white paper)," Ericsson, Stockholm, Sweden, Tech. Rep. 284 23-3149 Uen, 2011.
[3] CISCO, "CISCO visual networking Index: Global mobile data traffic forecast update, pp. 2016–2021 (white paper)," CISCO, San Jose, CA, USA, Tech. Rep. C11-481360-01, 2017.
[4] Nokia-Siemens-Networks, "2020: Beyond 4G radio evolution for the gigabit experience (white paper)," Nokia Siemens Netw., Espoo, Finland, Tech. Rep. C401-00722-WP-201106-1-EN, 2011.
[5] C.-X. Wang *et al.*, "Cellular architecture and key technologies for 5G wireless communication networks," *IEEE Commun. Mag.*, vol. 52, no. 2, pp. 122–130, Feb. 2014.
[6] I. Chih-Lin, C. Rowell, S. Han, Z. Xu, G. Li, and Z. Pan, "Toward green and soft: A 5G perspective," *IEEE Commun. Mag.*, vol. 52, no. 2, pp. 66–73, Feb. 2014.
[7] B. Bangerter, S. Talwar, R. Arefi, and K. Stewart, "Networks and devices for the 5G era," *IEEE Commun. Mag.*, vol. 52, no. 2, pp. 90–96, Feb. 2014.
[8] V. Sucasas, G. Mantas, and J. Rodriguez, "Security challenges for cloud radio access networks," in *Backhauling/Fronthauling for Future Wireless Systems*, K. M. S. Huq and J. Rodriguez, Eds. Hoboken, NJ, USA: Wiley, 2016, ch. 9, pp. 195–211.
[9] G. Mantas, N. Komninos, J. Rodriguez, E. Logota, and H. Marques, "Security for 5G Communications," in *Fundamentals 5G Mobile Networks*, J. Rodriguez, Ed. Hoboken, NJ, USA: Wiley, 2015, ch. 9, pp. 207–220.
[10] J. G. Andrews *et al.*, "What will 5G be?" *IEEE J. Sel. Areas Commun.*, vol. 32, no. 6, pp. 1065–1082, Jun. 2014.
[11] A. Radwan and J. Rodriguez, "Cloud of mobile small-cells for higher data-rates and better energy-efficiency," in *Proc. 23rd Eur. Wireless Conf.*, Dresden, Germany, May 2017, pp. 105–109.
[12] A. Asadi, Q. Wang, and V. Mancuso, "A survey on device-to-device communication in cellular networks," *IEEE Commun. Surveys Tuts.*, vol. 16, no. 4, pp. 1801–1819, Nov. 2014.
[13] Y. Zhang, E. Pan, L. Song, W. Saad, Z. Dawy, and Z. Han, "Social network aware device-to-device communication in wireless networks," *IEEE Trans. Wireless Commun.*, vol. 14, no. 1, pp. 177–190, Jan. 2015.
[14] C. Christophorou, A. Pitsillides, and I. Akyildiz, "CelEc framework for reconfigurable small cells as part of 5G ultra-dense networks," in *Proc. IEEE Int. Conf. Commun. (ICC)*, Paris, France, May 2017, pp. 1–7.
[15] D. Djenouri, L. Khelladi, and A. N. Badache, "A survey of security issues in mobile ad hoc and sensor networks," *IEEE Commun. Surveys Tuts.*, vol. 7, no. 4, pp. 2–28, 4th Quart., 2005.
[16] A. M. Hegland, E. Winjum, S. F. Mjolsnes, C. Rong, O. Kure, and P. Spilling, "A survey of key management in ad hoc networks," *IEEE Commun. Surveys Tuts.*, vol. 8, no. 3, pp. 48–66, 3rd Quart., 2006.
[17] J. van der Merwe, D. S. Dawoud, and S. McDonald, "A survey on peer-to-peer key management for mobile ad hoc networks," *ACM Comput. Surv.*, vol. 39, no. 1, 2007, Art. no. 1.
[18] E. D. Silva, A. L. D. Santos, L. C. P. Albini, and M. N. Lima, "Identity-based key management in mobile ad hoc networks: Techniques and applications," *IEEE Wireless Commun.*, vol. 15, no. 5, pp. 46–52, Oct. 2008.
[19] S. Zhao, A. Aggarwal, R. Frost, and X. Bai, "A survey of applications of identity-based cryptography in mobile ad-hoc networks," *IEEE Commun. Surveys Tuts.*, vol. 14, no. 2, pp. 380–400, 2nd Quart., 2012.
[20] M. Omar, Y. Challal, and A. Bouabdallah, "Certification-based trust models in mobile ad hoc networks: A survey and taxonomy," *J. Netw. Comput. Appl.*, vol. 35, no. 1, pp. 268–286, Jan. 2012.
[21] J. Liu, N. Kato, J. Ma, and N. Kadowaki, "Device-to-device communication in LTE-advanced networks: A survey," *IEEE Commun. Surveys Tuts.*, vol. 17, no. 4, pp. 1923–1940, 4th Quart., 2015.
[22] P. Mach, Z. Becvar, and T. Vanek, "In-band device-to-device communication in OFDMA cellular networks: A survey and challenges," *IEEE Commun. Surveys Tuts.*, vol. 17, no. 4, pp. 1885–1922, 4th Quart., 2015.
[23] M. Wang and Z. Yan, "A survey on security in D2D communications," *Mobile Netw. Appl.*, vol. 22, no. 2, pp. 195–208, Apr. 2017.
[24] D. Fang, Y. Qian, and R. Q. Hu, "Security for 5G mobile wireless networks," *IEEE Access*, vol. 6, pp. 4850–4874, 2018.
[25] R. Ahlswede, N. Cai, S.-Y. R. Li, and R. W. Yeung, "Network information flow," *IEEE Trans. Inf. Theory*, vol. 46, no. 4, pp. 1204–1216, Jul. 2000.
[26] M. de Ree, G. Mantas, A. Radwan, J. Rodriguez, and I. Otung, "Key management for secure network coding-enabled mobile small cells," in *Proc. Int. Conf. Broadband Commun., Netw. Syst.*,V. Sucasas, G. Mantas, and S. Althunibat, Eds. Faro, Portugal: Springer, vol. 263, 2018, pp. 327–336.
[27] S.-F. Chou, T.-C. Chiu, Y.-J. Yu, and A.-C. Pang, "Mobile small cell deployment for next generation cellular networks," in *Proc. IEEE Global Commun. Conf. (GLOBECOM)*, Austin, TX, USA, Dec. 2014, pp. 4852–4857.
[28] P. Swain, C. Christophorou, U. Bhattacharjee, C. M. Silva, and A. Pitsillides, "Selection of UE-based virtual small cell base stations using affinity propagation clustering," in *Proc. 14th Int. Wireless Commun. Mobile Comput. Conf. (IWCMC)*, Limassol, Cyprus, Jun. 2018, pp. 1104–1109.
[29] J. Rodriguez *et al.*, "SECRET—Secure network coding for reduced energy next generation mobile small cells: A european training network in wireless communications and networking for 5G," in *Proc. Internet Technol. Appl. (ITA)*, Wrexham, U.K., Sep. 2017, pp. 329–333.
[30] M. Haus, M. Waqas, A. Y. Ding, Y. Li, S. Tarkoma, and J. Ott, "Security and privacy in device-to-device (D2D) communication: A review," *IEEE Commun. Surveys Tuts.*, vol. 19, no. 2, pp. 1054–1079, 2nd Quart., 2017.
[31] A. Zhang and X. Lin, "Security-aware and privacy-preserving D2D communications in 5G," *IEEE Netw.*, vol. 31, no. 4, pp. 70–77, Jul./Aug. 2017.
[32] T. Chen, L. Wu, F. Wu, and S. Zhong, "Stimulating cooperation in vehicular ad hoc networks: A coalitional game theoretic approach," *IEEE Trans. Veh. Technol.*, vol. 60, no. 2, pp. 566–579, Feb. 2011.
[33] Z. Li and H. Shen, "Game-theoretic analysis of cooperation incentive strategies in mobile ad hoc networks," *IEEE Trans. Mobile Comput.*, vol. 11, no. 8, pp. 1287–1303, Aug. 2012.
[34] X. Chen, B. Proulx, X. Gong, and J. Zhang, "Exploiting social ties for cooperative d2d communications: A mobile social networking case," *IEEE/ACM Trans. Netw.*, vol. 23, no. 5, pp. 1471–1484, Oct. 2015.
[35] K. Zickuhr, "Location-based services," Pew Res. Center, Washington, DC, USA, Tech. Rep., 2013.
[36] A. Menezes, P. van Oorschot, and S. Vanstone, *Handbook of Applied Cryptography*, 5 ed. Boca Raton, FL, USA: CRC Press, 1996.
[37] D. R. Stinson, *Cryptography: Theory and Practice*. 3 ed. Boca Raton, FL, USA: CRC Press, 2005.
[38] A. Shamir, "Identity-based cryptosystems and signature schemes," in *Proc. CRYPTO*, G. R. Blakley and D. Chaum, Eds. Santa Barbara, CA, USA: Springer, vol. 196, 1984, pp. 47–53.
[39] D. Boneh and M. Franklin, "Identity-based encryption from the weil pairing," in *Proc. Annu. Int. Cryptol. Conf. (CRYPTO)* J. Kilian, Ed. Santa Barbara, CA, USA: Springer, vol. 2139, 2001, pp. 213–229.
[40] D. Boneh and M. Franklin, "Identity-based encryption from the Weil pairing," *SIAM J. Comput.*, vol. 32, no. 3, pp. 586–615, 2003.
[41] S. S. Al-Riyami and K. G. Paterson, "Certificateless public key cryptography," in *Proc. ASIACRYPT*, C.-S. Laih, Ed. Taipei, Taiwan: Springer, vol. 2894, 2003, pp. 452–473.
[42] A. W. Dent, "A brief introduction to certificateless encryption schemes and their infrastructures," in *Proc. Eur. Public Key Infrastruct. Workshop (EuroPKI)* F. Martinelli and B. Preneel, Eds. Pisa, Italy: Springer, vol. 6391, 2009, pp. 1–16.
[43] R. B. Bobba, L. Eschenauer, V. Gligor, and W. A. Arbaugh, "Bootstrapping security associations for routing in mobile ad-hoc networks," in *Proc. IEEE Global Telecommun. Conf. (GLOBECOM)*, San Francisco, CA, USA, vol. 3, Dec. 2003, pp. 1511–1515.
[44] S. H. Talawar, S. Maity, and R. C. Hansdah, "Secure routing with an integrated localized key management protocol in MANETs," in *Proc. IEEE 28th Int. Conf. Adv. Inf. Netw. Appl. (AINA)*, Victoria, BC, Canada, May 2014, pp. 605–612.
[45] K. Sanzgiri, B. Dahill, B. N. Levine, C. Shields, and E. M. Belding-Royer, "A secure routing protocol for ad hoc networks," in *Proc. 10th IEEE Int. Conf. Netw. Protocols (ICNP)*, Paris, France, Nov. 2002, pp. 78–87.
[46] P. Papadimitratos and H. J. Zygmunt, "Secure routing for mobile ad hoc networks," in *Proc. Commun. Netw. Distrib. Syst. Modelling Simulation Conf. (CNDS)*, San Antonio, TX, USA, 2002, pp. 193–204.
[47] Y.-C. Hu, D. B. Johnson, and A. Perrig, "SEAD: Secure efficient distance vector routing for mobile wireless ad hoc networks," *Ad Hoc Netw.*, vol. 1, no. 1, pp. 175–192, Jul. 2003.

[48] Y.-C. Hu, A. Perrig, and D. B. Johnson, "Ariadne: A secure on-demand routing protocol for ad hoc networks," *Wireless Netw.*, vol. 11, nos. 1–2, pp. 21–38, Jan. 2005.

[49] K. Sanzgiri, D. LaFlamme, B. Dahill, B. N. Levine, C. Shields, and E. M. Belding-Royer, "Authenticated routing for ad hoc networks," *IEEE J. Sel. Areas Commun.*, vol. 23, no. 3, pp. 598–610, Mar. 2005.

[50] C. Li, Z. Wang, and C. Yang, "Secure routing for wireless mesh networks," *Int. J. Netw. Secur.*, vol. 13, no. 2, pp. 109–120, Sep. 2011.

[51] S. Zhao, R. D. Kent, and A. Aggarwal, "An integrated key management and secure routing framework for mobile ad-hoc networks," in *Proc. 10th Annu. Int. Conf. Privacy, Secur. Trust (PST)*, Paris, France, Jul. 2012, pp. 96–103.

[52] S. Zhao, R. Kent, and A. Aggarwal, "A key management and secure routing integrated framework for mobile ad-hoc networks," *Ad Hoc Netw.*, vol. 11, no. 3, pp. 1046–1061, May 2013.

[53] J.-P. Hubaux and L. Buttyán, and S. Capkun, "The quest for security in mobile ad hoc networks," in *Proc. 2nd ACM Int. Symp. Mobile Ad Hoc Netw. Comput. (MobiHoc)*, Long Beach, CA, USA, Oct. 2001, pp. 146–155.

[54] S. Capkun, L. Buttyán, and J.-P. Hubaux, "Self-organized public-key management for mobile ad hoc networks," *IEEE Trans. Mobile Comput.*, vol. 2, no. 1, pp. 52–64, Jan./Mar. 2003.

[55] P. R. Zimmermann, *The Official PGP User's Guide*. Cambridge, MA, USA: MIT Press, 1995.

[56] K. Ren, T. Li, Z. Wan, F. Bao, R. H. Deng, and K. Kim, "Highly reliable trust establishment scheme in ad hoc networks," *Comput. Netw.*, vol. 45, no. 6, pp. 687–699, Aug. 2004.

[57] H. Kawabata, Y. Sueda, O. Mizuno, H. Nishikawa, and H. Ishii, "Self-organized key management based on trust relationship list," in *Proc. 12th Int. Conf. Intell. Next Gener. Netw. (ICIN)*, Oct. 2008, pp. 1–4.

[58] M. Omar, H. Boufaghes, L. Mammeri, A. Taalba, and A. Tari, "Secure and reliable certificate chains recovery protocol for mobile ad hoc networks," *J. Netw. Comput. Appl.*, vol. 62, pp. 153–162, Feb. 2016.

[59] R. Li, J. Li, H. Kameda, and P. Liu, "Localized public-key management for mobile ad hoc networks," in *Proc. IEEE Global Telecommun. Conf. (GLOBECOM)*, Dallas, TX, USA, vol. 2, Nov./Dec. 2004, pp. 1284–1289.

[60] R. 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, May 2006.

[61] Y. Kitada, A. Watanabe, I. Sasase, and K. Takemori, "On demand distributed public key management for wireless ad hoc networks," in *Proc. IEEE Pacific Rim Conf. Commun., Comput. Signal Process. (PACRIM)*, Victoria, BC, Canada, Aug. 2005, pp. 454–457.

[62] H. Mohri, I. Yasuda, Y. Takata, and H. Seki, "Certificate chain discovery in Web of trust for ad hoc networks," in *Proc. 21st Int. Conf. Adv. Inf. Netw. Appl. Workshops (AINAW)*, Niagara Falls, ON, Canada, vol. 2, May 2007, pp. 479–485.

[63] H. Mohri, I. Yasuda, Y. Takata, and H. Seki, "New certificate chain discovery methods for trust establishment in ad hoc networks and their evaluation," *Inf. Media Technol.*, vol. 3, no. 1, pp. 165–177, Mar. 2008.

[64] H. Dahshan and J. Irvine, "Key management in Web of trust for mobile ad hoc networks," in *Proc. Int. Conf. Adv. Inf. Netw. Appl. (AINA)*, Bradford, U.K., May 2009, pp. 363–370.

[65] H. Dahshan and J. Irvine, "On demand self-organized public key management for mobile ad hoc networks," in *Proc. IEEE 69th Veh. Technol. Conf. (VTC)*, Barcelona, Spain, Apr. 2009, pp. 1–5.

[66] H. Dahshan and J. Irvine, "A robust self-organized public key management for mobile ad hoc networks," *Secure Commun. Netw.*, vol. 3, no. 1, pp. 16–30, Jan./Feb. 2010.

[67] H. Dahshan and J. Irvine, "A robust and redundant key management for mobile ad hoc networks," in *Proc. 6th Int. Symp. Wireless Commun. Syst. (ISWCS)*, Sep. 2009, pp. 433–437.

[68] D. B. Johnson and D. A. Maltz, "Dynamic source routing in ad hoc wireless networks," in *Mobile Computing*, 1st ed. Boston, MA, USA: Springer, 1996, ch. 5, pp. 153–181.

[69] C. E. Perkins and E. M. Royer, "Ad-hoc on-demand distance vector routing," in *Proc. 2nd IEEE Workshop Mobile Comput. Syst. Appl. (WMCSA)*, New Orleans, LA, USA, Feb. 1999, pp. 90–100.

[70] E. C. H. Ngai and M. R. Lyu, "Trust- and clustering-based authentication services in mobile ad hoc networks," in *Proc. 24th Int. Conf. Distrib. Comput. Syst. Workshops (ICDCSW)*, Tokyo, Japan, Mar. 2004, pp. 582–587.

[71] E. C. H. Ngai, M. R. Lyu, and R. T. Chin, "An authentication service against dishonest users in mobile ad hoc networks," in *Proc. IEEE Aerosp. Conf.*, Big Sky, MT, USA, vol. 2, Mar. 2004, pp. 1275–1285.

[72] G. Hahn, T. Kwon, S. Kim, and J. Song, "Cluster-Based Certificate Chain for Mobile Ad Hoc Networks," in *Proc. Int. Conf. Comput. Sci. Appl. (ICCSA)*, M. L. Gavrilova, O. Gervasi, V. Kumar, C. J. K. Tan, D. Taniar, A. Laganá, Y. Mun, and H. Choo, Eds. Glasgow, U.K.: Springer, vol. 3981, 2006, pp. 769–778.

[73] C. Satizábal, J. Hernández-Serrano, J. Forné, and J. Pegueroles, "Building a virtual hierarchy to simplify certification path discovery in mobile ad-hoc networks," *Comput. Commun.*, vol. 30, no. 7, pp. 1498–1512, May 2007.

[74] G. Kambourakis, E. Konstantinou, and S. Gritzalis, "Binary tree based public-key management for mobile ad hoc networks," in *Proc. IEEE Int. Symp. Wireless Commun. Syst. (ISWCS)*, Reykjavik, Iceland, Oct. 2008, pp. 687–692.

[75] G. Kambourakis, E. Konstantinou, A. Douma, M. Anagnostopoulos, and G. Fotiadis, "Efficient certification path discovery for MANET," *EURASIP J. Wireless Commun. Netw.*, vol. 2010, Dec. 2010, Art. no. 243985.

[76] C.-P. Chang, J.-C. Lin, and F. Lai, "Trust-group-based authentication services for mobile ad hoc networks," in *Proc. 1st Int. Symp. Wireless Pervasive Comput. (ISWPC)*, Phuket, Thailand, Jan. 2006, pp. 1–4.

[77] S. Yi and R. Kravets, "Composite key management for ad hoc networks," in *Proc. 1st Annu. Int. Conf. Mobile Ubiquitous Syst., Netw. Services (MobiQuitous)*, Boston, MA, USA, Aug. 2004, pp. 52–61.

[78] J. Huang and D. Nicol, "A calculus of trust and its application to PKI and identity management," in *Proc. 8th Symp. Identity Trust Internet (IDtrust)*, Gaithersburg, MD, USA, Apr. 2009, pp. 23–37.

[79] H. Dahshan and J. Irvine, "A trust based threshold cryptography key management for mobile ad hoc networks," in *Proc. IEEE 70th Veh. Technol. Conf. Fall (VTC)*, Anchorage, AK, USA, pp. 1–5, Sep. 2009.

[80] M. Omar, Y. Challal, and A. Bouabdallah, "Reliable and fully distributed trust model for mobile ad hoc networks," *J. Comput. Secur.*, vol. 28, nos. 3–4, pp. 199–214, May/Jun. 2009.

[81] J. van der Merwe, D. S. Dawoud, and S. McDonald, "Trustworthy key management for mobile ad hoc networks," in *Proc. Southern Afr. Telecommun. Netw. Appl. Conf. (SATNAC)*, D. T. Browne, Ed., Stellenbosch, South-Africa, 2004, pp. 1–6.

[82] S. P. John and P. Samuel, "Self-organized key management with trusted certificate exchange in MANET," *Ain Shams Eng. J.*, vol. 6, no. 1, pp. 161–170, Mar. 2014.

[83] Y. L. Sun, W. Yu, Z. Han, and K. J. R. Liu, "Information theoretic framework of trust modeling and evaluation for ad hoc networks," *IEEE J. Sel. Areas Commun.*, vol. 24, no. 2, pp. 305–317, Feb. 2006.

[84] B. Bhargava *et al.*, "The pudding of trust," *IEEE Intell. Syst.*, vol. 19, no. 5, pp. 74–88, Sep./Oct. 2004.

[85] S. Čapkun, J.-P. Hubaux, and L. Buttyán, "Mobility helps security in ad hoc networks," in *Proc. 4th ACM Int. Symp. Mobile Ad Hoc Netw. Comput. (MobiHoc)*, Annapolis, MD, USA, Jun. 2003, pp. 46–56.

[86] 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, Jan. 2006.

[87] J. R. Douceur, "The Sybil Attack," in *Proc. Int. Workshop Peer-to-Peer Syst. (IPTPS)*, P. R. U. Druschel, F. Kaashoek, and A. Rowstron, Eds. Cambridge, MA, USA: Springer, vol. 2429, 2002, pp. 251–260.

[88] A. Irshad, S. M. Gilani, S. Khurram, M. Shafiq, A. W. Khan, and M. Usman, "Hash-chain based peer-peer key management and establishment of security associations in MANETS," in *Proc. Int. Conf. Inf. Emerg. Technol. (ICIET)*, Karachi, Pakistan, Jun. 2010, pp. 1–6.

[89] J. Kohl and C. Neuman, *The Kerberos Network Authentication Service (V5)*, document RFC-1510, Massachusetts Institute of Technology, Cambridge, MA, USA, 1993.

[90] M. Burrows, M. Adabi, and R. Needham, "A logic of authentication," DEC Syst. Res. Center, Palo Alto, CA, USA, Tech. Rep. 39, 1990.

[91] X. Li, S. Gordon, and J. Slay, "On demand public key management for wireless ad hoc networks," in *Proc. Austral. Telecommun. Netw. Appl. Conf. (ATNAC)*, Sydney, Australia, 2004, pp. 36–43.

[92] J. van der Merwe, D. Dawoud, and S. McDonald, "Fully self-organized peer-to-peer key management for mobile ad hoc networks," in *Proc. 4th ACM Workshop Wireless Secur. (WiSe)*, Cologne, Germany, Sep. 2005, pp. 21–30.

[93] L. Zhou and Z. J. Haas, "Securing ad hoc networks," *IEEE Netw.*, vol. 13, no. 6, pp. 24–30, Nov. 1999.

[94] L. Zhou, F. B. Schneider, and R. Van Renesse, "COCA: A secure distributed online certification authority," *ACM Trans. Comput. Syst.*, vol. 20, no. 4, pp. 329–368, Nov. 2002.
[95] L. Zhou, F. B. Schneider, R. Van Renesse, and Z. Haas, "Secure distributed on-line certification authority," U.S. Patent 10 001 588, Oct. 31, 2002.
[96] Y. G. Desmedt and Y. Frankel, "Threshold cryptosystems," in *Proc. CRYPTO*, G. Brassard, Ed., Santa Barbara, CA, USA: Springer, 1989, pp. 307–315.
[97] Y. G. Desmedt, "Threshold cryptography," *Eur. Trans. Telecommun.*, vol. 5, no. 4, pp. 449–458, Jul. 1994.
[98] A. Herzberg, S. Jarecki, H. Krawczyk, and M. Yung, "Proactive secret sharing OR: How to cope with perpetual leakage," in *Proc. CRYPTO*, Santa Barbara, CA, USA: Springer, 1995, pp. 339–352.
[99] S. Jarecki, "Proactive secret sharing public key cryptosystems," M.S. thesis, Dept. Elect. Eng. Comput. Sci., Massachusetts Inst. Technol., Cambridge, MA, USA, 1995.
[100] A. Herzberg, M. Jakobsson, S. Jarecki, H. Krawczyk, and M. Yung, "Proactive public key and signature systems," in *Proc. ACM Conf. Comput. Commun. Secur. (CCS)*, Zurich, Switserland, Apr. 1997, pp. 100–110.
[101] Y. Frankel, P. Gemmell, P. D. MacKenzie, and M. Yung, "Proactive RSA," in *Proc. CRYPTO*, B. S. Kaliski, Ed. Santa Barbara, CA, USA: Springer, pp. 440–454, 1997.
[102] Y. Frankel, P. Gemmell, P. D. MacKenzie, and M. Yung, "Optimal-resilience proactive public-key cryptosystems," in *Proc. 38th Annu. Symp. Found. Comput. Sci. (SFCS)*, Miami, FL, USA, Oct. 1997, pp. 384–393.
[103] P. Feldman, "A practical scheme for non-interactive verifiable secret sharing," in *Proc. 28th Annu. Symp. Found. Comput. Sci. (SFCS)*, Los Angeles, CA, USA, Oct. 1987, pp. 427–437.
[104] T. P. Pedersen, "Non-interactive and information-theoretic secure verifiable secret sharing," in *Proc. CRYPTO*, J. Feigenbaum, Ed. Santa Barbara, CA, USA: Springer, vol. 576, 1991, pp. 129–140.
[105] S. Yi and R. Kravets, "Key management for heterogeneous ad hoc wireless networks," Univ. Illinois at Urbana-Champaign, Champaign, IL, USA, Tech. Rep. UIUCDCS-R-2002-2290, 2002.
[106] S. Yi and R. Kravets, "Key management for heterogeneous ad hoc wireless networks," in *Proc. 10th IEEE Int. Conf. Netw. Protocols (ICNP)*, Paris, France, pp. 202–203, Nov. 2002.
[107] S. Yi and R. Kravets, "MOCA: MObile certificate authority for wireless ad hoc networks," Univ. Illinois Urbana-Champaign, Champaign, IL, USA, Tech. Rep. UIUCDCS-R-2004-2502, 2004.
[108] S. Yi and R. Kravets, "MOCA: MObile certificate authority for wireless ad hoc networks," in *Proc. 2nd PKI Res. Workshop (PKI)*, Gaithersburg, MD, USA, 2003, pp. 79–93.
[109] H. N. Nguyen and H. Morino, "A key management scheme for mobile ad hoc networks based on threshold cryptography for providing fast authentication and low signaling load," in *Proc. 1st Int. Workshop Secur. Ubiquitous Comput. Syst. (SecUbiq)*, T. Enokido, L. Yan, B. Xiao, D. Kim, Y. Dai, and L. T. Yang, Eds. vol. 3823, Nagasaki, Japan: Springer, 2005, pp. 905–915.
[110] B. Wu, J. Wu, E. B. Fernandez, and S. Magliveras, "Secure and efficient key management in mobile ad hoc networks," in *Proc. 19th IEEE Int.Parallel Distrib. Process. Symp. (IPDPS)*, Denver, CO, USA, Apr. 2005, pp. 1–8.
[111] B. Wu, J. Wu, E. B. Fernandez, M. Ilyas, and S. Magliveras, "Secure and efficient key management in mobile ad hoc networks," *J. Netw. Comput. Appl.*, vol. 30, no. 3, pp. 937–954, Aug. 2007.
[112] Y. Guo, J. Ma, C. Wang, and L. Wang, "Mechanism design based nodes selection model for threshold key management in MANETs," in *Proc. IEEE 11th Int. Conf. Trust, Secur. Privacy Comput. Commun. (TRUSTCOM)*, Liverpool, U.K., 2012, pp. 303–309.
[113] Y. Guo, J. Ma, C. Wang, and K. Yang, "Incentive-based optimal nodes selection mechanism for threshold key management in MANETs with selfish nodes," *Int. J. Distrib. Sensor Netw.*, vol. 9, no. 5, pp. 1–13, May 2013.
[114] Q. Chen, X. Lin, S. Shen, K. Hashimoto, and N. Kato, "A group-based key management protocol for mobile ad hoc networks," in *Proc. IEEE Global Telecommun. Conf. (GLOBECOM)*, Honolulu, HI, USA, Nov./Dec. 2009, pp. 4305–4309.
[115] Q. Chen, Z. M. Fadlullah, X. Lin, and N. Kato, "A clique-based secure admission control scheme for mobile ad hoc networks (MANETs)," *J. Netw. Comput. Appl.*, vol. 34, no. 6, pp. 1827–1835, Nov. 2011.
[116] M. Girault, "Self-certified public keys," in *Proc. EUROCRYPT*, D. W. Davies, Ed. vol. 547, Brighton, U.K.: Springer, pp. 490–497, 1991.
[117] J. van der Merwe, D. S. Dawoud, and S. McDonald, "A public key management scheme and threshold- multisignature scheme for mobile ad hoc networks," *South Afr. Inst. Electr. Eng.*, vol. 97, no. 1, pp. 82–92, Jan. 2006.
[118] R. Ostrovsky and M. Yung, "How to withstand mobile virus attacks," in *Proc. 10th ACM Symp. Princ. Distrib. Comput. (PODC)*, Montreal, QC, Canada, Aug. 1991, pp. 51–59.
[119] M. Ge and K.-Y. Lam, "Self-healing key management service for mobile ad hoc networks," in *Proc. 1st Int. Conf. Ubiquitous Future Netw. (ICUFN)*, Hong Kong, Jun. 2009, pp. 177–182.
[120] P. Khatri, S. Tapaswi, and U. P. Verma, "Trust evaluation in wireless ad hoc networks using fuzzy system," in *Proc. CUBE Int. Inf. Technol. Conf. (CUBE)*, Pune, India, Sep. 2012, pp. 779–783.
[121] P. Khatri, "Using identity and trust with key management for achieving security in ad hoc networks," in *Proc. IEEE Int. Advance Comput. Conf. (IACC)*, Gurgaon, India, Feb. 2014, pp. 271–275.
[122] M. Bechler, H.-J. Hof, D. Kraft, F. Pahlke, and L. Wolf, "A cluster-based security architecture for ad hoc networks," in *Proc. IEEE Int. Conf. Comput. Commun. (INFOCOM)*, Hong Kong, Mar. 2004, pp. 2393–2403.
[123] W. Rao and S. Xie, "Merging clustering scheme in distributed certificate authority for ad hoc network," in *IET Int. Conf. Wireless, Mobile Multimedia Netw. (ICWMMN)*, Hangzhou, China, 2006, pp. 1–4.
[124] Y. Dong, H. W. Go, A.-F. Sui, V. O. K. Li, L. C.-K. Hui, and S. M. Yiu, "Providing distributed certificate authority service in mobile ad hoc networks," in *Proc. 1st Int. Conf. Secur. Privacy Emerg. Areas Commun. Netw. (SECURECOMM)*, Athens, Greece, Sep. 2005, pp. 149–156.
[125] Y. Dong, A.-F. Sui, S. M. Yiu, V. O. K. Li, and L. C.-K. Hui, "Providing distributed certificate authority service in cluster-based mobile ad hoc networks," *Comput. Commun.*, vol. 30, nos. 11–12, pp. 2442–2452, Sep. 2007.
[126] A. Z. Ghalwash, A. A. A. Youssif, S. M. Hashad, and R. Doss, "Self adjusted security architecture for mobile ad hoc networks (MANETs)," in *Proc. 6th IEEE/ACIS Int. Conf. Comput. Inf. Sci. (ICIS)*, Melbourne, Australia, Jul. 2007, pp. 682–687.
[127] G. Xu and L. Iftode, "Locality driven key management architecture for mobile ad-hoc networks," in *IEEE Int. Conf. Mobile Ad-hoc Sensor Syst.*, Fort Lauderdale, FL, USA, Oct. 2004, pp. 436–446.
[128] L. Xu, X. Wang, and J. Shen, "Strategy and simulation of trust cluster based key management protocol for ad hoc networks," in *Proc. 4th Int. Conf. Comput. Sci. Educ. (ICCSE)*, Nanning, China, 2009, pp. 269–274.
[129] H. Dahshan and J. Irvine, "An elliptic curve distributed key management for mobile ad hoc networks," in *Proc. IEEE 71st Veh. Technol. Conf. (VTC)*, Taipei, Taiwan, May 2010, pp. 1–5.
[130] H. Dahshan and J. Irvine, "A threshold key management scheme for mobile ad hoc networks using elliptic curve dlog-based cryptosystem," in *Proc. 8th Annu. Commun. Netw. Services Res. Conf. (CNSR)*, Montreal, QC, Canada, May 2010, pp. 130–137.
[131] H. Dahshan and J. Irvine, "An elliptic curve secret sharing key management scheme for mobile ad hoc networks," *Secur. Commun. Netw.*, vol. 4, no. 12, pp. 1405–1419, Dec. 2011.
[132] Q. S. Liu, D. S. Zhang, and Y. Zhao, "Study on framework of distributed key management for MANETs," in *Proc. Int. Conf. Inf. Netw. Secur. (ICINS)*, Beijing, China, pp. 1–6, Nov. 2013.
[133] N. Koblitz, "Elliptic curve cryptosystems," *Math. Comput.*, vol. 48, no. 177, pp. 203–209, 1987.
[134] A. Khalili, J. Katz, and W. A. Arbaugh, "Toward secure key distribution in truly ad-hoc networks," in *Proc. Symp. Appl. Internet Workshops (SAINT)*, Orlando, FL, USA, Jun. 2003, pp. 342–346.
[135] M. Ge, K.-Y. Lam, D. Gollmamnn, 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, Sep. 2009.
[136] Z. Zhang, W. Susilo, and R. Raad, "Mobile ad-hoc network key management with certificateless cryptography," in *Proc. 2nd Int. Conf. Signal Process. Commun. Syst. (ICSPCS)*, Gold Coast, QLD, Australia, Dec. 2008, pp. 1–10.
[137] H. Luo and S. Lu, "Ubiquitous and robust authentication services for ad hoc wireless networks," Univ. California, Los Angeles, CA, USA, Tech. Rep. UCLA-CSD-TR-200030, 2000.
[138] J. Kong, P. Zerfos, H. Luo, S. Lu, and L. Zhang, "Providing robust and ubiquitous security support for mobile ad-hoc networks," in *Proc. 9th Int. Conf. Netw. Protocols (ICNP)*, Riverside, CA, USA, Nov. 2001, pp. 251–260.

[139] H. Luo, P. Zerfos, J. Kong, S. Lu, and L. Zhang, "Self-securing ad hoc wireless networks," in *Proc. 7th IEEE Int. Symp. Comput. Commun. (ISCC)*, Taormina, Italy, Nov. 2002, pp. 567–574.

[140] H. Luo, J. Kong, P. Zerfos, S. Lu, and L. Zhang, "URSA: Ubiquitous and robust access control for mobile ad hoc networks," *IEEE/ACM Trans. Netw.*, vol. 12, no. 6, pp. 1049–1063, Dec. 2004.

[141] M. Stadler, "Publicly verifiable secret sharing," in *Proc. EUROCRYPT*, U. Maurer, Ed. Saragossa, Spain: Springer, vol. 1070, pp. 190–199, 1996.

[142] B. Schoenmakers, "A simple publicly verifiable secret sharing scheme and its application to electronic voting," in *Proc. CRYPTO*, M. Wiener, Ed. Santa Barbara, CA, USA: Springer, vol. 1666, pp. 148–164, 1999.

[143] M. Narasimha, G. Tsudik, and J. H. Yi, "On the utility of distributed cryptography in P2P and MANETs: The case of membership control," in *Proc. 11th IEEE Int. Conf. Netw. Protocols (ICNP)*, Atlanta, GA, USA, Nov. 2003, pp. 336–345.

[144] A. Balasubramanian, S. Mishra, and R. Sridhar, "A hybrid approach to key management for enhanced security in ad hoc networks," Univ. Buffalo, Buffalo, NY, USA, Tech. Rep. 2004-09, 2004.

[145] A. Balasubramanian, S. Mishra, and R. Sridhar, "Analysis of a hybrid key management solution for ad hoc networks," in *Proc. IEEE Wireless Commun. Netw. Conf.*, vol. 4, New Orleans, LA, USA, Mar. 2005, pp. 2082–2087.

[146] B. Zhu, F. Bao, R. H. Deng, M. S. Kankanhalli, and G. Wang, "Efficient and robust key management for large mobile ad hoc networks," *Comput. Netw.*, vol. 48, no. 4, pp. 657–682, Jul. 2005.

[147] C.-H. Lin and C.-Y. Lee, "Modified autonomous key management scheme with reduced communication/computation costs in MANET," in *Proc. Int. Conf. Complex, Intell. Softw. Intensive Syst. (CISIS)*, Krakow, Poland, Feb. 2010, pp. 818–821.

[148] C.-H. Lin, C.-Y. Lee, and D.-J. Chen, "Modified autonomous key management scheme with reduced communication/ computation costs in MANET," *Comput. Inf.*, vol. 30, no. 6, pp. 1167–1180, 2011.

[149] M. A. Azad, S. Bag, S. Parkinson, and F. Hao, "TrustVote: Privacy-preserving node ranking in vehicular networks," *IEEE Internet Things J.*, to be published.

[150] S. Raghani, D. Toshniwal, and R. Joshi, "Dynamic support for distributed certification authority in mobile ad hoc networks," in *Proc. Int. Conf. Hybrid Inf. Technol. (ICHIT)*, Cheju Island, South Korea, vol. 1, 2006, pp. 424–432.

[151] K. Hamouid and K. Adi, "Robust key management scheme for certification in mobile ad-hoc networks," in *Proc. 14th IEEE Int. Symp. Comput. Commun. (ISCC)*, Sousse, Tunisia, Jul. 2009, pp. 355–360.

[152] M. Ge, K.-Y. Lam, J. Li, and S.-L. Chung, "Ubiquitous and secure certificate service for mobile ad hoc network," in *Proc. 5th IEEE/IFIP Int. Conf. Embedded Ubiquitous Comput. (EUC)*, Shanghai, China, vol. 2, pp. 312–317, Dec. 2008.

[153] M. Ge, K.-Y. Lam, J.-B. Li, and S.-L. Chung, "Ubiquitous and secure certificate service for wireless ad hoc network," *IEICE Trans. Inf. Syst.*, vol. 93, no. 7, pp. 1848–1856, Jul. 2010.

[154] B. Lynn, "Authenticated identity-based encryption," unpublished.

[155] W. He, Y. Huang, K. Nahrstedt, and W. C. Lee, "SMOCK: A scalable method of cryptographic key management for mission-critical networks," Univ. Illinois Urbana-Champaign, Champaign, IL, USA, Tech. Rep. UIUCDCS-R-2006-2734, 2006.

[156] W. He, Y. Huang, R. Sathyam, K. Nahrstedt, and W. C. Lee, "SMOCK: A scalable method of cryptographic key management for mission-critical wireless ad-hoc networks," *IEEE Trans. Inf. Forensics Security*, vol. 4, no. 1, pp. 140–150, Mar. 2009.

[157] S. P. John and P. Samuel, "A distributed hierarchical key management scheme for mobile Ad hoc networks," in *Proc. Int. Conf. Inf., Netw. Automat. (ICINA)*, vol. 1, Kunming, China, Oct. 2010, pp. 308–314.

[158] S. P. John and P. Samuel, "A predictive clustering technique for effective key management in mobile ad hoc networks," *Inf. Secur. J., A Global Perspective*, vol. 20, nos. 4–5, pp. 250–260, Oct. 2011.

[159] R. Gennaro, S. Jarecki, H. Krawczyk, and T. Rabin, "Secure distributed key generation for discrete-log based cryptosystems," in *Proc. EUROCRYPT*, J. Stern, Ed., vol. 1592, Prague, Czech Republic: Springer, 1999, pp. 295–310.

[160] Y. Zhang, W. Liu, W. Lou, Y. Fang, and Y. Kwon, "AC-PKI: Anonymous and certificateless public-key infrastructure for mobile ad hoc networks," in *Proc. IEEE Int. Conf. Commun. (ICC)*, Seoul, South-Korea, vol. 5, 2005, pp. 3515–3519.

[161] G. Li and W. Han, "A new scheme for key management in ad hoc networks," in *Proc. 4th Int. Conf. Netw. (ICN)*, P. Lorenz and P. Dini, Eds., Reunion Island, France: Springer, vol. 3421, 2005, pp. 242–249.

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

[163] J. Li, D. Wei, and H. Kou, "Identity-based and threshold key management in mobile ad hoc networks," in *Proc. Int. Conf. Wireless Commun., Netw. Mobile Comput. (WiCOM)*, Wuhan, China, Sep. 2006, pp. 1–4.

[164] L. Wei, C.-R. Zhang, and L.-Q. Zheng, "A key management scheme based generalized signcryption in mobile ad hoc network," in *Proc. Int. Conf. Commun. Intell. Inf. Secur. (ICCIIS)*, Nanning, China, Oct. 2010, pp. 117–120.

[165] F. R. Yu, H. Tang, P. C. Mason, and F. Wang, "A hierarchical identity based key management scheme in tactical mobile ad hoc networks," *IEEE Trans. Netw. Service Manage.*, vol. 7, no. 4, pp. 258–267, Dec. 2010.

[166] Y. Zhang, W. Liu, and W. Lou, "Anonymous communications in mobile ad hoc networks," in *Proc. IEEE Int. Conf. Comput. Commun. (INFOCOM)*, Miami, FL, USA, vol. 3, Mar. 2005, pp. 1940–1951.

[167] F. R. Yu, H. Tang, F. Wang, and V. C. M. Leung, "Distributed node selection for threshold key management with intrusion detection in mobile ad hoc networks," in *Proc. 12th IEEE Int. Conf. Comput. Sci. Eng. (CSE)*, Vancouver, BC, Canada, vol. 2, Aug. 2009, pp. 787–794.

[168] F. R. Yu and H. Tang, "Distributed node selection for threshold key management with intrusion detection in mobile ad hoc networks," *Wireless Netw.*, vol. 16, no. 8, pp. 2169–2178, Nov. 2010.

[169] N. Saxena, G. Tsudik, and J. H. Yi, "Identity-based access control for ad hoc groups," in *Proc. 7th Int. Conf. Inf. Secur. Cryptol. (ICISC)*, C.-S. Park and S. Chee, Eds. Seoul, South-Korea: Springer, vol. 3506, 2004, pp. 362–379.

[170] L.-C. Li and R.-S. Liu, "Securing cluster-based ad hoc networks with distributed authorities," *IEEE Trans. Wireless Commun.*, vol. 9, no. 10, pp. 3072–3081, Oct. 2010.

[171] H. Deng, A. Mukherjee, and D. P. Agrawal, "Threshold and identity-based key management and authentication for wireless ad hoc networks," in *Proc. Int. Conf. Inf. Technol., Coding Comput. (ITCC)*, Las Vegas, NV, USA, vol. 1, Apr. 2004, pp. 107–111.

[172] H. Deng and D. P. Agrawal, "TIDS: Threshold and identity-based security scheme for wireless ad hoc networks," *Ad Hoc Netw.*, vol. 2, no. 3, pp. 291–307, Jul. 2004.

[173] B. Wang and J. Li, "(t,n) Threshold Signature Scheme Without a Trusted Party," *Chin. J. Comput.*, vol. 26, no. 11, pp. 1581–1584, 2003.

[174] P. Xia, M. Wu, K. Wang, and X. Chen, "Identity-based fully distributed certificate authority in an OLSR MANET," in *Proc. 4th Int. Conf. Wireless Commun., Netw. Mobile Comput. (WiCOM)*, Dalian, China, Oct. 2008, pp. 1–4.

[175] H.-C. Lin, M.-K. Sun, H.-T. Lin, and W.-C. Kuo, "Multi-level and group-based key management for mobile ad hoc networks," in *Proc. Int. Conf. Inf. Secur. Intell. Control (ISIC)*, Yunlin, Taiwan, Aug. 2012, pp. 164–167.

[176] A. C.-F. Chan, "Distributed private key generation for identity based cryptosystems in ad hoc networks," *IEEE Wireless Commun. Lett.*, vol. 1, no. 1, pp. 46–48, Feb. 2012.

[177] H. Sun, X. Zheng, and Z. Deng, "An identity-based and threshold key management scheme for ad hoc networks," in *Proc. Int. Conf. Netw. Secur., Wireless Commun. Trusted Comput. (NSWCTC)*, Wuhan, China, vol. 2, Apr. 2009, pp. 520–523.

[178] Y. Ren, J. Wang, Y. Zhang, and L. Fang, "Identity-based key issuing protocol for ad hoc networks," in *Proc. 3rd Int Conf. Comput. Intell. Secur. (CIS)*, Harbin, China, Dec. 2007, pp. 917–921.

[179] Y. Zhang, J. Liu, Y. Wang, J. Han, H. Wang, and K. Wang, "Identity-based threshold key management for ad hoc networks," in *Proc. IEEE Pacific–Asia Workshop Comput. Intell. Ind. Appl. (PACIIA)*, Wuhan, China, vol. 2, pp. 797–801, Dec. 2008.

[180] L. Harn and C. Lin, "Strong (n,t,n) verifiable secret sharing scheme," *Inf. Sci.*, vol. 180, no. 16, pp. 3059–3064, Aug. 2010.

[181] E. Da Silva and L. C. P. Albini, "Towards a fully self-organized identity-based key management system for MANETs," in *Proc. IEEE 9th Int. Conf. Wireless Mobile Comput., Netw. Commun. (WiMob)*, Lyon, France, Oct. 2013, pp. 717–723.

[182] N. Saxena, "Public key cryptography sans certificates in ad hoc networks," in *Proc. 4th Int.Conf. Appl. Cryptogr. Netw. Secur. (ACNS)*, J. Zhou, M. Yung, and F. Bao, Eds. Singapore: Springer, vol. 3989, 2006, pp. 375–389.

[183] F. Li, M. Shirase, and T. Takagi, "Key management using certificateless public key cryptography in ad hoc networks," in *Proc. 5th IFIP Int. Conf. Netw. Parallel Comput. (NPC)*, J. Cao, M. Li, M.-Y. Wu, and J. Chen, Eds. Shanghai, China: Springer, vol. 5245, 2008, pp. 116–126.
[184] J. Baek, R. Safavi-Naini, and W. Susilo, "Certificateless public key encryption without pairing," in *Proc. 8th Int. Conf. Inf. Secur. (ISC)*, J. Zhou, J. Lopez, R. H. Deng, and F. Bao, Eds. Singapore: Springer, vol. 3650, 2005, pp. 134–148.
[185] J. Lai and W. Kou, "Self-generated-certificate public key encryption without pairing," in *Proc. Int. Workshop Public Key Cryptogr. (PKC)*, T. Okamoto and X. Wang, Eds. Beijing, China: Springer, vol. 4450, 2007, pp. 476–489.
[186] A. Shamir, "How to share a secret," *Commun. ACM*, vol. 22, no. 11, pp. 612–613, Nov. 1979.
[187] X. Lv, H. Li, and B. Wang, "Identity-Based Key Distribution for Mobile Ad Hoc Networks," *Frontiers Comput. Sci. China*, vol. 5, no. 4, pp. 442–447, Dec. 2011.
[188] X. Lv, H. Li, and B. Wang, "Virtual private key generator based escrow-free certificateless public key cryptosystem for mobile ad hoc networks," *Secur. Commun. Netw.*, vol. 6, no. 1, pp. 49–56, Jan. 2013.
[189] L. Li, Z. Wang, W. Liu, and Y. Wang, "A certificateless key management scheme in mobile ad hoc networks," in *Proc. 7th Int. Conf. Wireless Commun., Netw. Mobile Comput. (WiCOM)*, Wuhan, China, Sep. 2011, pp. 1–4.
[190] S. Khatoon and B. S. Thakur, "Certificate less key management scheme in manet using threshold cryptography," *Int. J. Netw. Secur. Appl.*, vol. 7, no. 2, pp. 55–59, Mar. 2015.
[191] T. Eissa, S. A. Razak, and M. A. Ngadi, "A novel lightweight authentication scheme for mobile ad hoc networks," *Arabian J. Sci. Eng.*, vol. 37, no. 8, pp. 2179–2192, Dec. 2012.
[192] S. Kasra-Kermanshahi and M. Salleh, "An enhanced certificateless cryptosystem for mobile ad hoc networks," in *Proc. Int. Symp. Biometrics Secur. Technol. (ISBAST)*, Kuala Lumpur, Malaysia, Aug. 2014, pp. 176–181.
[193] S. Kasra-Kermanshahi and M. Salleh, "An improved certificateless public key authentication scheme for mobile ad hoc networks over elliptic curves," in *Pattern Analysis, Intelligent Security and the Internet of Things* , vol. 355, A. Abraham, A. K. Muda, and Y.-H. Choo, Eds. Malacca, Malaysia: Springer, 2015, pp. 327–334.
[194] S. Kasra-Kermanshahi and M. Salleh, "Certificateless public key cryptosystems for mobile ad hoc networks," *Int. J. Sci. Res. Sci., Eng. Technol. (IJRSET)*, vol. 1, no. 1, pp. 176–183, 2015.
[195] T. P. Pedersen, "A threshold cryptosystem without a trusted party," in *Proc. EUROCRYPT*, D. W. Davies, Ed. Brighton, U.K.: Springer, vol. 547, 1991, pp. 522–526.
[196] B. Chor, S. Goldwasser, S. Micali, and B. Awerbuch, "Verifiable secret sharing and achieving simultaneity in the presence of faults," in *Proc. 26th Annu. Symp. Found. Comput. Sci. (SFCS)*, Portland, OR, USA, pp. 383–395, Oct. 1985.
[197] J. Zheng, S. Xu, F. Zhao, D. Wang, and Y. Li, "A novel detective and self-organized certificateless key management scheme in mobile ad hoc networks," in *Proc. IEEE Int. Conf. Granular Comput. (GrC)*, Beijing, China, Dec. 2013, pp. 443–448.
[198] Z. Moradlu, M. A. Doostari, M. Gharib, and A. Movaghar, "Fully distributed self certified key management for large-scale MANETs," in *Proc. IEEE 10th Int. Conf. Ubiquitous Intell. Comput. and IEEE 10th Int. Conf. Autonomic Trusted Comput. (ATC'13)*, Vietri sul Mere, Italy, Dec. 2013, pp. 96–102.
[199] M. Gharib, Z. Moradlu, M. A. Doostari, and A. Movaghar, "Fully distributed ECC-based key management for mobile ad hoc networks," *Comput. Netw.*, vol. 113, pp. 269–283, Feb. 2017.
[200] J. Daemen and V. Rijmen, *The Design of Rijndael: AES—The Advanced Encryption Standard*. Berlin, Germany: Springer, 2002.
[201] R. Blom, "An optimal class of symmetric key generation systems," in *Proc. EUROCRYPT*, T. Beth, N. Cot, and I. Ingemarsson, Eds. Paris, France: Springer, vol. 209, 1984, pp. 335–338.
[202] T. Matsumoto and H. Imai, "On the key predistribution system: A practical solution to the key distribution problem," in *Proc. CRYPTO*, C. Pomerance, Ed. Santa Barbara, CA, USA: Springer, vol. 293, 1987, pp. 185–193.
[203] C. Blundo, A. de Santis, A. Herzberg, S. Kutten, U. Vaccaro, and M. Yung, "Perfectly-secure key distribution for dynamic conferences," in *Proc. CRYPTO*, E. F. Brickell, Ed. Santa Barbara, CA, USA: Springer, vol. 740, pp. 471–486, 1992.
[204] L. Eschenauer and V. D. Gligor, "A key-management scheme for distributed sensor networks," in *Proc. 9th ACM Conf. Comput. Commun. Secur. (CCS)*, Washington, DC, USA, Nov. 2002, pp. 41–47.
[205] H. Chan, A. Perrig, and D. Song, "Random key predistribution schemes for sensor networks," in *Proc. IEEE Symp. Secur. Privacy (SP)*, Berkeley, CA, USA, 2003, pp. 197–213.
[206] A. C.-F. Chan, "Distributed symmetric key management for mobile ad hoc networks," in *Proc. IEEE Int. Conf. Comput. Commun. (INFOCOM)*, Hong Kong, vol. 4, pp. 2414–2424, 2004.
[207] A. C.-F. Chan, "Probabilistic distributed key predistribution for mobile ad hoc networks," in *Proc. IEEE Int. Conf. Commun. (ICC)*, Paris, France, vol. 6, Jun. 2004, pp. 3743–3747.
[208] L. Goratti, G. Steri, K. M. Gomez, and G. Baldini, "Connectivity and security in a D2D communication protocol for public safety applications," in *Proc. 11th Int. Symp. Wireless Commun. Syst. (ISWCS)*, Barcelona, Spain, Aug. 2014, pp. 548–552.
[209] J. Wu and R. Wei, "Comments on "distributed symmetric key management for mobile ad hoc networks,"" *Inf. Process. Lett.*, vol. 109, no. 14, pp. 822–824, Jun. 2009.
[210] C. K. Wong, M. Gouda, and S. S. Lam, "Secure group communications using key graphs," *IEEE/ACM Trans. Netw.*, vol. 8, no. 1, pp. 16–30, Feb. 2000.
[211] J. Staddon, S. Miner, M. Franklin, D. Balfanz, M. Malkin, and D. Dean, "Self-healing key distribution with revocation," in *Proc. IEEE Symp. Secur. Privacy (SP)*, Berkeley, CA, USA, May 2002, pp. 241–257.
[212] D. Liu, P. Ning, and K. Sun, "Efficient self-healing group key distribution with revocation capability," in *Proc. 10th ACM Conf. Comput. Commun. Secur. (CCS)*, Washington, DC, USA, Oct. 2003, pp. 231–240.
[213] B. Rong, H. H. Chen, Y. Qian, K. Lu, R. Q. Hu, and S. Guizani, "A pyramidal security model for large-scale group-oriented computing in mobile ad hoc networks: The key management study," *IEEE Trans. Veh. Technol.*, vol. 58, no. 1, pp. 398–408, Jan. 2009.
[214] M. Alam, D. Yang, J. Rodriguez, and R. Abd-alhameed, "Secure device-to-device communication in LTE-A," *IEEE Commun. Mag.*, vol. 52, no. 4, pp. 66–73, Apr. 2014.
[215] N.-C. Wang and S.-Z. Fang, "A Hierarchical Key Management Scheme for Secure Group Communications in Mobile Ad Hoc Networks," *J. Syst. Softw.*, vol. 80, no. 10, pp. 1667–1677, Oct. 2007.
[216] W. Shen, W. Hong, X. Cao, B. Yin, D. M. Shila, and Y. Cheng, "Secure key establishment for Device-to-Device communications," in *Proc. 33rd IEEE Global Telecommun. Conf. (GLOBECOM)*, Austin, TX, USA, Dec. 2014, pp. 336–340.
[217] M. Pužar, J. Andersson, T. Plagemann, and Y. Roudier, "SKiMPy: A simple key management protocol for MANETs in emergency and rescue operations," in *Proc. 2nd Eur.Conf. Secur. Privacy Ad-Hoc Sensor Netw. (ESAS)*, R. Molva, G. Tsudik, and D. Westhoff, Eds. Visegrad, Hungary: Springer, vol. 3813, 2005, pp. 14–26.
[218] F. Hao, X. Yi, L. Chen, and S. F. Shahandashti, "The fairy-ring dance: Password authenticated key exchange in a group," in *Proc. 1st ACM Workshop IoT Privacy, Trust, Secur. (IoTPTS)*, Singapore, Apr. 2015, pp. 1–8.
[219] T.-C. Chiang and Y.-M. Huang, "Group keys and the multicast security in ad hoc networks," in *Proc. 32nd Int. Conf. Parallel Process. Wksp. (ICPPW)*, Kaohsiung, Taiwan, Oct. 2003, pp. 385–390.
[220] H.-Y. Chien and R.-Y. Lin, "Identity-based key agreement protocol for mobile ad-hoc networks using bilinear pairing," in *Proc. IEEE Int. Conf. Sensor Netw., Ubiquitous, Trustworthy Comput. (SUTC)*, Taichung, Taiwan, vol. 1, Jun. 2006, pp. 520–529.
[221] H.-Y. Chien and R.-Y. Lin, "Improved ID-based security framework for ad hoc network," *Ad Hoc Netw.*, vol. 6, no. 1, pp. 47–60, Jan. 2008.
[222] B. Wu, J. Wu, and Y. Dong, "An efficient group key management scheme for mobile ad hoc networks," *Int. J. Secur. Netw.*, vol. 4, nos. 1–2, pp. 125–134, Feb. 2008.
[223] Y. Jung, E. Festijo, and M. Peradilla, "Joint operation of routing control and group key management for 5G ad hoc D2D networks," in *Proc. Int. Conf. Privacy Secur. Mobile Syst. (PRISMS)*, Aalborg, Denmark, May 2014, pp. 1–8.
[224] S. Agrawal and D. Boneh, "Homomorphic MACs: MAC-based integrity for network coding," in *Proc. 7th Int.Conf. Appl. Cryptogr. Netw. Secur. (ACNS)*, M. Abdalla, D. Pointcheval, P.-A. Fouque, and D. Vergnaud, Eds. Paris, France: Springer, 2009, pp. 292–305.

[225] P. Zhang, Y. Jiang, C. Lin, H. Yao, A. Wasef, and X. Shen, "Padding for orthogonality: Efficient subspace authentication for network coding," in *Proc. IEEE Int. Conf. Comput. Commun.(INFOCOM)*, Shanghai, China, Apr. 2011, pp. 1026–1034.
[226] D. Yang, A. Esfahani, G. Mantas, and J. Rodriguez, "Jointly padding for subspace orthogonality against tag pollution," in *Proc. IEEE 19th Int. Workshop Comput. Aided Modeling Design Commun. Links Netw. (CAMAD)*, Athens, Greece, Dec. 2014, pp. 85–89.
[227] A. Esfahani, D. Yang, G. Mantas, A. Nascimento, and J. Rodriguez, "An improved homomorphic message authentication code scheme for RLNC-enabled wireless networks," in *Proc. IEEE 19th Int. Workshop Comput. Aided Modeling Design Commun. Links Netw. (CAMAD)*, Athens, Greece, Dec. 2014, pp. 80–84.
[228] A. Esfahani, G. Mantas, D. Yang, A. Nascimento, J. Rodriguez, and J. C. Neves, "Towards secure network coding enabled wireless sensor networks in cyber-physical systems," in *Cyber-Physical Systems: From Theory to Practice* D. B. Rawat, J. Rodrigues, and I. Stojmenovic, Eds., 1st ed. Boca Raton, FL, USA: CRC Press, 2015, pp. 395–414.
[229] A. Esfahani, D. Yang, G. Mantas, A. Nascimento, and J. Rodriguez, "Dual-homomorphic message authentication code scheme for network coding-enabled wireless sensor networks," *Int. J. Distrib. Sensor Netw.*, vol. 11, no. 7, Jul. 2015, Art. no. 510251.
[230] A. Esfahani, G. Mantas, J. Rodriguez, A. Nascimento, and J. C. Neves, "A null space-based MAC scheme against pollution attacks to random linear network coding," in *Proc. IEEE Int. Conf. Commun. Workshop (ICCW)*, London, U.K., Jul. 2015, pp. 1521–1526.
[231] A. Esfahani, G. Mantas, H. Silva, J. Rodriguez, and J. C. Neves, "An efficient MAC-based scheme against pollution attacks in XOR network coding-enabled WBANs for remote patient monitoring systems," *EURASIP J. Wireless Commun. Netw.*, vol. 2016, no. 113, Dec. 2016.
[232] A. Esfahani, G. Mantas, and J. Rodriguez, "An efficient null space-based homomorphic MAC scheme against tag pollution attacks in RLNC," *IEEE Commun. Lett.*, vol. 20, no. 5, pp. 918–921, May 2016.

MARCUS DE REE received the B.Eng. degree in applied mathematics from The Hague University of Applied Sciences, The Netherlands, in 2012, and the M.Sc. degree in applied mathematics of communication systems from San Diego State University, USA, in 2017. He is currently pursuing the Ph.D. degree in electronic engineering with the University of South Wales, U.K.

Since 2017, he has been an Early Stage MSCA Researcher of the EU-funded SECRET Project and a member of the 4TELL Research Group, Instituto de Telecomunicações, Aveiro, Portugal. His research interests include cryptography, secure wireless communication, decentralized systems, and coding theory.

Mr. de Ree has served as a Program Committee Member and a Reviewer for the BROADNETS'18 conference. He was a recipient of the H/Link Thesis Award for the Most Newsworthy Thesis, in 2013.

GEORGIOS MANTAS (M'07) received the Diploma degree in electrical and computer engineering from the University of Patras, Greece, in 2005, the M.Sc. degree in information networking from Carnegie Mellon University, PA, USA, in 2008, and the Ph.D. degree in electrical and computer engineering from the University of Patras, in 2012.

In 2014, he became a Postdoctoral Researcher at the Instituto de Telecomunicações, Aveiro, Portugal, where he has been involved in research projects, such as ECSEL—SemI40, CATRENE—MobiTrust, CATRENE—NewP@ss, ARTEMIS—ACCUS, FP7—CODELANCE, and FP7—SEC-SALUS. Since 2018, he has been a Lecturer with the University of Greenwich, U.K. His main research interests include network and system security, authentication mechanisms, privacy-preserving mechanisms, intrusion detection systems, and secure network coding.

AYMAN RADWAN (SM'15) received the M.A.Sc. degree from Carleton University, Ottawa, Canada, and the Ph.D. degree from Queen's University, Kingston, Canada.

He is currently a Senior Research Engineer and the EU Project Manager with the Instituto de Telecomunicações (Institute of Telecommunications), Aveiro, Portugal, where he is mainly working in the areas of 5G and mobile communications. Since 2010, he has been intensively active in European projects, coordinating and technically managing multiple EU projects. He was the Technical Manager of the FP7 Project C2POWER and the Coordinator of the CELTIC Project Green-T. He is also the Coordinator of the CELTIC Plus Project MUSCLES and the Project Manager of the H2020 ITN-SECRET. He is also an expert in the field of 5G and future mobile communications, with specific concentration on radio resource management and green communications. His recent research interest includes the Internet of Things, specifically e-health and intelligent transportation systems.

SHAHID MUMTAZ (M'13) received the M.Sc. degree in electrical and electronic engineering from the Blekinge Institute of Technology (BTH) Karlskrona, Sweden, in 2006, and the Ph.D. degree in electrical and electronic engineering from the University of Aveiro, Portugal, in 2011. His M.Sc. and Ph.D. degrees were funded by the Swedish Government and FCT Portugal.

He has more than ten years of wireless industry experience. He was a Research Intern with Ericsson and Huawei Research Labs, Karlskrona, Sweden, in 2005. He is currently a Senior Research Scientist and the Technical Manager with the Instituto de Telecomunicações (IT), Aveiro, Portugal. He has been involved in several EC R&D Projects in the field of green communication and next-generation wireless systems. In EC projects, he holds the position of the Technical Manager, where he oversees the project from a scientific and technical side, managing all details of each work packages, which gives the maximum impact of the project's results for the further development of commercial solutions. He has been also involved in two Portuguese-funded projects (SmartVision and Mobilia) in the areas of networking coding and development of system-level simulator for the 5G wireless systems. He has several years of experience in 3GPP radio systems research with experience in HSPA/LTE/LTE-A and strong track record in relevant technology field, especially physical layer technologies, LTE cell planning and optimization, protocol stack, and system architecture. His research interests include the fields of architectural enhancements to 3GPP networks (i.e., LTE-A user plan and control plan protocol stack, NAS, and EPC), 5G NR-related technologies, green communications, cognitive radio, cooperative networking, radio resource management, network slicing, LAA/LTU, cross-layer design, backhaul/fronthaul, heterogeneous networks, M2M and D2D communication, and baseband digital signal processing. He has more than 150 publications in international conferences, journal papers, and book chapters.

JONATHAN RODRIGUEZ (SM'13) received the master's degree in electronic and electrical engineering and the Ph.D. degree from the University of Surrey, U.K., in 1998 and 2004, respectively.

In 2005, he became a Researcher at the Instituto de Telecomunicações, Portugal, and acquired Senior status, in 2008. In 2009, he became an Invited Assistant Professor at the University of Aveiro, Portugal, and an Associate Professor, in 2015. He has served as the Project Coordinator for major international research projects, including Eureka LOOP and FP7 C2POWER, while acting as the Technical Manager for FP7 COGEU and FP7 SALUS. In 2017, he became a Professor of mobile communications at the University of South Wales, U.K. He is currently leading the H2020-ETN SECRET project, a European Training Network on 5G communications. He is the author of more than 480 scientific works that include ten book editorials.

Dr. Rodriguez has been a Chartered Engineer (CEng), since 2013, and a Fellow of the IET, since 2015. In 2018, he became an Associate Editor of the *IET Communications* journal.

IFIOK E. OTUNG received the B.Sc. (Hons.) and M.Sc. degrees in electronic and electrical engineering from the University of Ife, Nigeria, and the Ph.D. degree in satellite communications from the University of Surrey, U.K.

He is currently a Professor of satellite communications with the University of South Wales (USW, formerly University of Glamorgan). Since 1997, he has been with USW, where he teaches courses on satellite, mobile, and digital communications and has supervised around 120 postgraduate projects, including M.Sc. and Ph.D. He is also a Chartered Engineer with broad and international experience of research and teaching at various universities in Europe and Africa. He founded and continues to manage the popular M.Sc. in mobile and satellite communications at USW.