SeDS: Secure Data Sharing Strategy for D2D Communication in LTE-Advanced Networks

Aiqing Zhang, *Student Member, IEEE*, Jianxin Chen, *Member, IEEE*,
Rose Qingyang Hu, *Senior Member, IEEE*, and Yi Qian, *Senior Member, IEEE*

***Abstract*—Security and availability are two crucial issues in device-to-device (D2D) communication, with its fast development in fourth-generation (4G) Long-Term Evolution Advanced (LTE-Advanced) networks. In this paper, we propose a secure data sharing protocol, which merges the advantages of public key cryptography and symmetric encryption, to achieve data security in D2D communication. Specifically, a public-key-based digital signature, combined with a mutual authentication mechanism of a cellular network, guarantees entity authentication, transmission nonrepudiation, traceability, data authority, and integrity. Meanwhile, symmetric encryption is employed to ensure data confidentiality. A salient feature of the proposed protocol is that it can detect free-riding attack by keeping a record of the current status for user equipment (UE) and realize reception nonrepudiation by key hint transmission between the UE and evolved NodeB, thus improving system availability. Furthermore, various delay models are established in different application scenarios to seek the optimal initial service providers (SPs) for achieving tradeoff between cost and availability. Extensive analysis and simulations demonstrate that the proposed protocol is indeed an efficient and practical solution for a secure data sharing mechanism for D2D communication.**

***Index Terms*—Availability, data sharing, device-to-device (D2D) communication, Long-Term Evolution Advanced (LTE-A) network, security.**

Manuscript received January 22, 2014; revised July 14, 2014 and December 6, 2014; accepted March 18, 2015. Date of publication March 23, 2015; date of current version April 14, 2016. This work was supported in part by the State Key Development Program of Basic Research of China under Grant 2013CB329005; by the National Natural Science Foundation of China under Grant 61322104, Grant 61201165, Grant 61271240, and Grant 61401228; by the Priority Academic Program Development of Jiangsu Higher Education Institutions; by the Nanjing University of Posts and Telecommunications Foundation under Grant NY211032; by the Education Natural Science Foundation of Jiangsu Province under Grant 13KJB510026; and by the Innovation Program for Postgraduate of Jiangsu Province under Grant KYLX-0811. The review of this paper was coordinated by Dr. J. Pan.

A. Zhang is with the Key Laboratory of Broadband Wireless Communication and Sensor Network Technology, Ministry of Education, Nanjing University of Posts and Telecommunications, Nanjing 210003, China, and also with Anhui Normal University, Anhui 241000, China (e-mail: aqzhang2006@163.com).

J. Chen is with the Key Laboratory of Broadband Wireless Communication and Sensor Network Technology, Ministry of Education, Nanjing University of Posts and Telecommunications, Nanjing 210003, China (e-mail: chenjx@njupt.edu.cn).

R. Q. Hu is with the Department of Electrical and Computer Engineering, Utah State University, Logan, UT 84322-4120 USA (e-mail: rosehu@ieee.org).

Y. Qian is with the Department of Electrical and Computer Engineering, University of Nebraska–Lincoln, Omaha, NE 68182-0572 USA (e-mail: yqian2@unl.edu).

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TVT.2015.2416002

I. Introduction

RECENT years have witnessed a tremendous growth of the mobile user population and multimedia services, which is causing a severe traffic overload problem in traditional cellular networks. Device-to-device (D2D) communication has been proposed as a promising data offloading solution and spectrum efficiency enhancement method due to its inherent characteristics, e.g., improving resource utilization, enhancing user's throughput, extending battery lifetime, etc. [1]–[5]. Accordingly, it has drawn considerable attention in research community in recent years. In addition to the conventional cellular operation where user equipment units (UEs) are served directly by the evolved NodeB (eNB), UEs are also able to communicate directly with each other over the D2D link [5]. Different from the traditional D2D communication techniques such as Bluetooth or Wi-Fi direct, D2D communication underlaying Long-Term Evolution Advanced (LTE-A) networks works on a licensed band, which usually provides a planned deployment instead of an uncoordinated one, resulting in a better user experience and quality-of-service guarantee. Therefore, it is necessary and important to develop new functions and applications with the assistance of cellular networks.

Unfortunately, despite its obvious advantages, D2D communication still faces two substantial technical challenges when applied to large-scale applications, i.e., security and availability. As the connections happen directly between the proximity devices, D2D communication may subject to many security threats such as modification and fabrication of the data, violation of the user privacy, and so on. Evidently, any malicious behavior of users may cause serious consequence and lead to deteriorated user experience. Furthermore, availability must be achieved in the sense that users might be unhappy if the services are intermittent or they suffer from a long waiting time for sharing the information. As a result, it is ultimately important to develop some elaborate and carefully designed protocols to achieve security and availability in D2D communication before its practical implementations. However, as far as we know, very limited work has been proposed to address the given issues in D2D communication.

To bridge the gap between the elegant theory and realistic application, in this paper, we aim at addressing the problem of security assurance for data transmission in D2D communications. Specifically, we introduce a secure data sharing protocol (SeDS) through a cryptographic approach, in which both public-key-based signature and symmetric encryption are applied to realize the security objectives. In particular, the data shared among the

legitimate users is signed by the data provider to ensure data authority, and the signed data will be re-signed by the transmitter to guarantee transmission nonrepudiation and to offer evidence for the data sharing event, which is employed to resist free-riding attack and improve system availability. By jointly considering the characteristics of the cellular network and the digital signature, traceability is ensured with a simple secure one-way hash function, which is efficient in computation and communication overhead. Meanwhile, a symmetric encryption technique, which is time and energy efficient compared with the asymmetric method, is adopted to protect the original information from leaking out. To decrypt the data, the receiver is expected to send a key hint request message to the eNB, thus achieving reception nonrepudiation, which is an important feature of the proposed protocol. In summary, our contributions are threefold.

First, we propose a SeDS in D2D communication environment. With the help of SeDS, the resources shared among the users are confidentiality and integrity assured through end-to-end encryption. In addition, if the transmitted data do not originated from the authorized provider or altered by some adversaries, the receiver is able to detect the event by signature verification and report a feedback message to the manager. Thus, the fabricated message can be stopped from influencing other users.

Second, to improve the availability of SeDS protocol, we set a record table in eNB for free-riding detection, thus leading to peers' cooperation in relaying message. Simultaneously, the record table is employed to guarantee traceability by referring the pseudoidentity to the corresponding real identity (RID). Moreover, various models are established to estimate delay under different application scenarios for selecting the minimal number of initial service providers (SPs), which are selected to strike a balance between the cost and availability.

Finally, we analyze the security characteristics in detail and evaluate the SeDS performance of communication cost, computation cost, and availability altogether.

The remainder of this paper is organized as follows. An overview on the related work is conducted in Section II. Background and preliminaries of the proposed protocol are presented in Section III. In Section IV, the proposed protocol is formed and discussed in detail, followed by security analysis in Section V. Section VI evaluates the performance of the proposed protocol through extensive simulations. Finally, Section VII concludes this paper.

II. Related Work

Extensive studies have been reported on D2D communication as an underlay to LTE-A networks. However, most of them have focused on resource allocation and interference management or mode selection [6]–[10], whereas not much effort has been made on security issues [11]–[13]. Specifically, instead of interference mitigation and avoidance, in [12], interference against eavesdropping were exploited, which is an effective way to enhance information-theoretic secrecy capacity. This paper is heuristic, although it does not consider the security requirements of D2D pairs. In [13], a coalitional game-theoretic framework was developed to devise social-tie-based cooperation strategies for D2D communication and establishes a new D2D cooperation paradigm by leveraging two social phenomena, i.e., social trust and social reciprocity, which is a promising direction for treating security problems in D2D communication. However, this paper does not consider and analyze the potential threats such as eavesdropping or fabricating.

The most related studies similar to this paper are the security mechanisms in wireless body area networks (WBANs) and vehicle ad hoc networks (VANETs) because they have very similar network features with D2D communication systems with some small differences. Then, we review the main security approaches in WBANs and VANETs for a comprehensive understanding of the security strategies in different wireless communication environments, which cultivate an insight into our proposed protocol.

In WBANs, considering the stringent energy and memory constraints, symmetric cryptography is widely studied in terms of key management [14], data transmission protocol [15], [16], and access control [17]. However, ever increasing interest has been raised in exploring the feasibility of implementation of asymmetric encryption in wireless sensor networks aiming at improving the security level by taking the advantage of the public key cryptography [18]. The encouraging results depend on bilinear pairing, which is also the preliminary of our proposed protocol. In VANETs, the energy constraint is not as vital as that in WBANs, whereas the time efficiency is considered a critical constraint. As public key infrastructure (PKI) satisfies most VANET security requirements, it is the most viable mechanism in terms of secure data transmission [19], [20], conditional privacy [21], [22], and authentication [23]. The comparisons of security issues in D2D, WBANs, and VANETs are listed in Table I.

As the cellular network has full control over the D2D connections, we may take the advantage of this special feature to simplify the protocol and achieve the demanding security requirements. Generally, UEs and eNB perform mutual authentication on a cellular path, which should be used in D2D mode as well so that the entities can be freed up from the complicated authentication process as implemented in VANETs. Furthermore, key exchange commitment may be finished before the data transmission events occur, instead of time-consuming key predistribution as in WBANs. However, availability, which is not intensively investigated in the aforementioned networks, is a very critical security requirement in D2D communication. By jointly considering these points, we attempt to design a secure data sharing protocol in D2D communication by mixing digital signature and symmetric encryption to achieve a good security performance.

III. System Model

A. Network Architecture

To capture a general D2D communication scenario, similar to [2], here we consider a typical music concert scenario. Suppose that the organizers promise to provide the audience with concert video information. They only need to put up the media server, which is installed at the hall and registered to the cellular

TABLE I
SECURITY APPROACHES AND OBJECTIVES COMPARISON

System		PKI	Symmetric encryption	Security objectives
D2D	[12]	×	×	Secrecy capacity and eavesdropping resist
	[13]	×	×	Cooperation promotion
WBANs	[14]	×	√	Resilience to adversary intervention and network configurations
	[15]	×	√	Privacy preservation and access control
	[16]	×	√	Symmetric key generation based on physiological signals
	[17]	×	√	Privacy preservation and authentication
	[18]	√	√	Content oriented and contextual privacy, forging attack resist
VANETs	[19]	√	×	Privacy preservation and cooperative data forwarding
	[20]	√	√	Data security, collisions and hidden terminal avoidance
	[21]	√	×	Sybil attack mitigation and privacy preservation
	[22]	√	×	Privacy preservation, traceability and replication
	[23]	√	√	Anonymous authentication and traceability

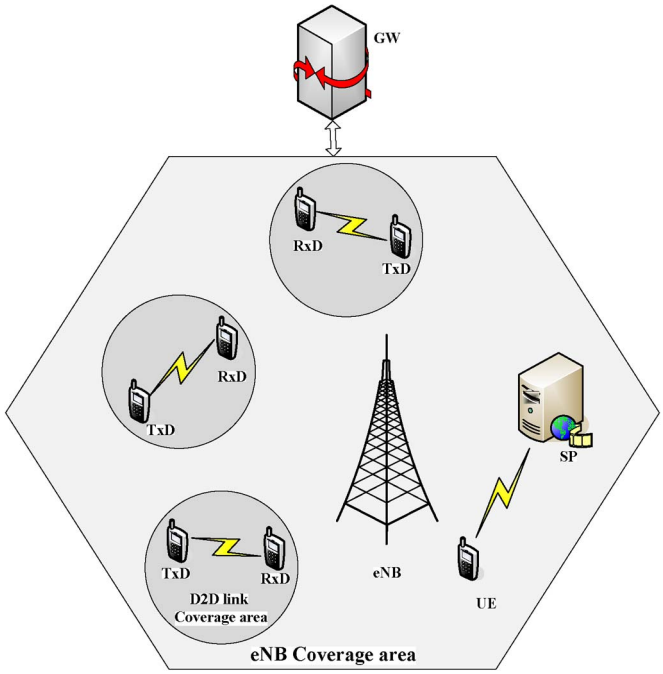

Fig. 1. System model for a general D2D communication scenario.

network. Thus, the participators can download or share the data with their mobile phones using D2D communications.[1]

Extensively, a D2D communication system includes four parts: gateway (GW) and eNB of a cellular network, the UEs of cellular users, and server of an SP. Their relationship is shown in Fig. 1.

GW: GW serves as the gate from the local subsystem to the core network. In addition to routing Internet Protocol packets from/to the Internet, the GW is able to detect the potential D2D traffic with the proximity service control function (PSCF). The PSCF earmarks the traffic flows and looks for pairs of D2D enabled devices.

eNB: eNB, which is the infrastructure connected to the mobile phone network and the GW, is a very important element in Evolved Universal Terrestrial Radio Access (E-UTRA) of the LTE-A network. It is responsible for resource allocation of cellular networks and coordination of devices by ensuring two peers meet in space, time, and frequency. The eNB also controls the transmit power of the cellular users to limit the interference and implements user authentication in cellular networks. Additionally, in our security system, eNB acts as the trust authority, to which the UEs and SP register. It usually possesses not only high storage capacity but also strong computational capacity.

UEs: UEs[2] are the peer entities of the D2D connections. The information available at the devices is shared among users by D2D communications without increasing additional traffic load to the cellular network. Assume all the UEs in our system are within the communication radius of the same serving eNB. Note that in the LTE-A network, UE is designed with the function of mutual authentication with the eNB.

SP: SP is proposed to provide authentic information at the beginning of the system establishment process. The information should be sent to partial UEs so that they can then share the data with other devices by D2D links. When most of the UEs obtain the material, SP does not necessary continue to serve.

In the system, eNB and GW are assumed completely trustable and cannot be comprised by the attackers. Moreover, SP is honest enough to provide correct source data, whereas UEs may be comprised of or captured by some adversaries, the threats of which are analyzed in the following.

B. Threat Model and Security Requirements

Generally, D2D communication is wireless, which may introduce a number of security vulnerabilities, including *eavesdropping*, *data fabrication or alternation*, *privacy violation*, and *denial-of-service (DoS) attacks*. DoS attacks on wireless communication networks have been extensively investigated over the past decades [24], [25]. Thus, we will focus on the other security issues in D2D communications. In particular, there may exist some UEs which receive data from their pairs, while not being willing to share the resource with others since the data transmission process is energy-consuming. Such selfish behavior is referred to as a free-riding attack, which causes a serious threat and reduces the system availability of D2D communication.

To mitigate the potential threats, the proposed protocol is desired to achieve security objectives considering *data confidentiality authority and correctness*, *entity authentication*, and

[1]We consider media sharing scenario for the ease of the understanding. This special scenario can be extended to be more general.

[2]In most D2D communication systems, UEs refer to mobile phones, which are ubiquitous handheld devices with functionalities varying from communication of voice and data to transmission of video streaming.

TABLE II
NOTATIONS AND DESCRIPTION

Notation	Description	Notation	Description
TA	Trust Authority	X_i	The public key of UE_i or SP
SP	Service Provider	x_i	The private key of UE_i or SP
UE_i	The ith User Equipment	$H_0()$	A secure hash function such as $\{0,1\}^* \rightarrow \mathbb{Z}_q^*$
k	The security parapmeter	$H_1()$	A secure hash function such as $\{0,1\}^* \rightarrow \mathbb{G}$
RID_i	Real identity of UE_i or SP	$Enc_s()$	Symmetric encryption algorithm with key s
PID_i	Pseudo identity of UE_i or SP	$Dec_s()$	Symmetric decryption algorithm with key s
P_i	The portion index of data	$a\|\|b$	String concatenation of a and b

privacy preservation. Simultaneously, *nonrepudiation* is necessary to prevent legitimate users from denying transmission or reception of their messages. To achieve this security objective, the digital signature is usually adopted, which is efficient in transmission nonrepudiation but failing to deal with reception nonrepudiation. Therefore, a carefully designed protocol is expected to resist reception nonrepudiation. Moreover, *availability* is an important requirement as users may be frustrated if services become temporarily unavailable due to the attacks such as free-riding or DoS. The system availability features are also influenced by the time period that the users wait for services in D2D communication.

C. Preliminaries

The bilinear pairing and Diffle–Hellman key exchange (DHKE) are the basis of our proposed scheme. Hence, we briefly review related definition here. (For a more detailed introduction, see [26]).

Bilinear pairing: Let $\mathbb{G}$ and $\mathbb{G}_T$ be two multiplicative cyclic groups of the same prime order q. Let g and g_1 be two generators of $\mathbb{G}$ and $\mathbb{G}_T$, respectively. A mapping $\hat{e} : \mathbb{G} \times \mathbb{G} \rightarrow \mathbb{G}_T$ is called an admissible bilinear map if it satisfies the following properties.

1) Bilinear: For all $V, Q \in \mathbb{G}$ and $a, b \in \mathbb{Z}_q^*$, we have $\hat{e}(V^a, Q^b) = \hat{e}(V, Q)^{ab}$.
2) Symetric: $\hat{e}(V, Q) = \hat{e}(Q, V)$.
3) Nondegenerate: $\hat{e}(V, Q) \neq 1_{\mathbb{G}_T}$, where $V, Q \neq 1_{\mathbb{G}}$.
4) Computable: $\hat{e}$ is efficiently computable.

As mentioned in [27], such an admissible map can be constructed by the modified Weil of Tate pairing on elliptic curve and a 160-bit prime order q is assumed to reach an 80-bit security level.

Definition 1 Bilinear Parameter Generator Gen: A bilinear parameter generator Gen is a probabilistic algorithm that takes a security parameter k as input and outputs a tuple $(q, g, g_1, \mathbb{G}, \mathbb{G}_T, \hat{e})$, where $\mathbb{G}$ and $\mathbb{G}_T$ are two multiplicative cyclic groups of order q. g and g_1 are two generators of $\mathbb{G}$ and $\mathbb{G}_T$, and $\hat{e} : \mathbb{G} \times \mathbb{G} \rightarrow \mathbb{G}_T$ is an admissible bilinear map.

Diffie-Hellman Key Exchange: DHKE [28], which is based on Discrete logarithm problem (DLH) [29], provides a practical solution to the key distribution problem, i.e., it enables two parties to derive a common secret key by communicating over an unsecured channel. The basic idea underlying DHKE is that the exponentiation in $\mathbb{Z}_q^*$ is a one-way function and commutative, i.e.,

$$k = (x^a)^b \equiv (x^b)^a \mod q.$$

The value k is the joint secret that can be used as the session key between two parties, in which $A = x^a$ and $B = x^b$ are named key hints. Then, two parties only need to exchange their key hints, and the secret key can be computed separately (due to space limitations, see [28] for more detailed illustration).

IV. PROPOSED PROTOCOL

We consider integrating PKI-based signature and symmetric key encryption to achieve security goals in D2D communication. Digital signature is employed to realize entity authentication and data authority. Alternatively, symmetric key encryption is expected to ensure data confidentiality. For clarity of presentation, the notations used throughout this paper are listed in Table II.

A. System Initialization

System Parameter Generation: The trust authority eNB, given the security parameter k, generates the tuple $(q, g, g_1, \mathbb{G}, \mathbb{G}_T, \hat{e})$ by running $Gen(k)$. Then, the eNB chooses one secure symmetric encryption algorithm $\text{Enc}_s()$ and two hash functions H_0 and H_1, where $H_0 : \{0,1\}^* \rightarrow \mathbb{Z}_q^*$, H_1: $\{0,1\}^* \rightarrow \mathbb{G}$. Finally, the system parameters $\text{params} = (q, g, g_1, \mathbb{G}, \mathbb{G}_T, \hat{e}, \text{Enc}_s(), H_0, H_1)$ are published.

SP Registration: The SP, with RID RID_0, registers to the system for providing the original data in the system. The eNB first computes $\text{PID}_0 = H_0(\text{RID}_0)$ as pseudoidentity for SP. Then, it randomly selects an integer $x_0 \in \mathbb{Z}_q^*$ as the private key and sets the public key for the SP by $X_0 = g^{x_o}$. Finally, the eNB sends the public/private key (X_0, x_0) pair to the SP through a secure channel.

UE Registration: When UE_i registers to the system with RID RID_i (e.g., the SIM card number), the eNB sets $\text{PID}_i = H_0(\text{RID}_i)$ as the pseudoidentity for the entity. Then, it randomly selects an integer $x_i \in \mathbb{Z}_q^*$ as the private key and computes the public key for UE_i by $X_i = g^{x_i}$. The public/private key (X_i, x_i) is sent to the UE_i via a secure channel. Meanwhile, the tuple (X_0, PID_0) is also sent to the register. Thus, the device joins the system and becomes the legitimate member. Note that

TABLE III
MEMBER RECORD IN eNB

RID	PID	Pubilic key	Portion index (P_i)	Share frequency	Malicious behavior amount
RID_0	PID_0	X_0	$0, 1, 2, \cdots p$	0	0
RID_1	PID_1	X_1	0	0	0
RID_2	PID_2	X_2	0	0	0
$\cdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$

TABLE IV
MESSAGE FORMAT IN SP

Portion index (P_i)	Payload (M)	Signature (σ_1)
2 Bytes	L Bytes	20 Bytes

the SP and UEs compute their pseudoidentities by themselves for reducing communication overhead.[3]

System Setup: The eNB keeps a record of the status for the entities and the frequency that they share the data with their counterparts, as shown in Table III. As the data may be divided into several frames if it is too large (e.g., video clips), "Portion index (P_i)" is introduced in the system to index the data.[4] The item "Share frequency" counts the amounts that the device transmits data to their neighbors. "Malicious behavior amount" records the number of times the entity transmits fake or fabricated message. It is evident that all the initial values are "0." Meanwhile, for the verification of the original data, the eNB stores the material M and the corresponding portion index as well. Additionally, to guarantee data authority and integrity, the data shared between peers is a packet signed by the SP, who is the original and authentic provider of the service. The signature process is designed to be completed offline to reduce the data sharing latency. Specifically, The SP computes the signature

$$\sigma_1 = H_1(P_i \| M)^{x_0}. \tag{1}$$

Remark 1: The signature process in VANETs and WBAN, e.g., the algorithm in literature [15], [20], and [22], may be far more complex for realizing traceability and Sybil mitigation, whereas in our system, these targets are attained by converging identity authentication in cellular mode and record table verification in the proposed protocol, which largely facilitates the signature formation and reduces computational cost accordingly. It is the same case for the signature of Step 5.

With P_i indexing the material, the SP stores the data in the format of Table IV.

B. Secure Data Sharing Protocol

As the system has been initialized, here, we concentrate on how the data are shared among the users with security and availability. The secure data sharing protocol is shown in Fig. 2, and the processes are presented by the following steps.

Step 1 Service Request: A UE (called UE$_i$), who intends to get the ith frame of the data, randomly selects $c \in \mathbb{Z}_q^*$ and computes the key hint $z = g^c$ for generation of communication key k_c, which is used for encryption to ensure the data confidentiality. Additionally, for the message integrity and authentication, we introduce HMAC specified as Internet standard RFC 2104 in the protocol. The HMAC for message m is hash value by computing

$$\text{HMAC}_k(m) = h\left[(k^+ \oplus \text{opad}) \| h\left[(k^+ \oplus \text{ipad}) \| m\right]\right] \tag{2}$$

where k^+ is the key padded out to size, $opad = 0011\ 0110$, $0011\ 0110, \ldots, 0011\ 0110$ and ipad $= 0101\ 1100, 0101\ 1100$, $\ldots, 0101\ 1100$ are specified padding constants, and $h(\cdot)$ is a cryptographic hash functions such as SHA-1.

Then, UE$_i$ sends a service request message along with its PID$_i$, z, and the expected portion index P_i, namely $(\text{PID}_i \| z \| P_i \| h[(k^+ \oplus \text{opad}) \| h[(k^+ \oplus \text{ipad}) \| \text{PID}_i \| z \| P_i]])$, to the eNB.

Remark 2:

1) For the simplification of expression, $h[(k^+ \oplus \text{opad}) \| h[(k^+ \oplus ipad) \| \text{PID}_i \| z \| P_i]]$ is expressed as $h(\bullet, x_i)$, where $\bullet$ denotes the message attached by the HMAC. The other HMACs in the next steps and Fig. 2 are expressed as the same formation.
2) In the HMAC, the key x_i is hashed together with the message. Note that the key x_i is known and only known by the sender UE$_i$ and receiver eNB. If the message is modified, the hashed value computed by the receiver will be unequal to the hashed value received. Then, the modification can be detected.

Step 2 Authentication: Upon receiving the request message, the eNB first verifies its integrity and verification by computing hashed value of the message[5] and authenticates the requester in the normal cellular communication mode, obtaining the RID (i.e., the SIM card number of the cell phone) RID$_i$. Then, it refers to the record Table III to check if the PID$_i$ sent by UE$_i$ and RID$_i$ are one-to-one map. If so, it continues examining the UE$_i$'s portion index in the record table. If the request portion exists in the record, the message is ignored. Otherwise, the eNB will forward request message with RID$_i$[6] to the GW for detecting the traffic and finding out the transmitter candidates.

Step 3 Candidate Detection: The PSCF in the GW performs the proximity service detection and searches the potential D2D pairs for the requesting UE.[7] Then, the GW responds the eNB with the RIDs of candidates.

[3]For simplicity of expression, $(X_i, x_i), i = 0, 1, 2, \ldots$ is applied to represent the public/private key for SP and UE in the remainder of this paper.

[4]Suppose the original material is divided into p portions; thus, P_i may be $0, 1, 2, \ldots, p$. Note the number "0" represents the entity getting no share.

[5]In the later steps, all the receivers will perform this procedure to check the message integrity and message authentication. To shorten the space, we omit this procedure in the next steps.

[6]Suppose the security communication between the eNB and GW is guaranteed by a normal cellular network.

[7]In our paper, as we are concentrated on security issues, see [2] and the references therein for more specific illustration for proximity discovery processes.

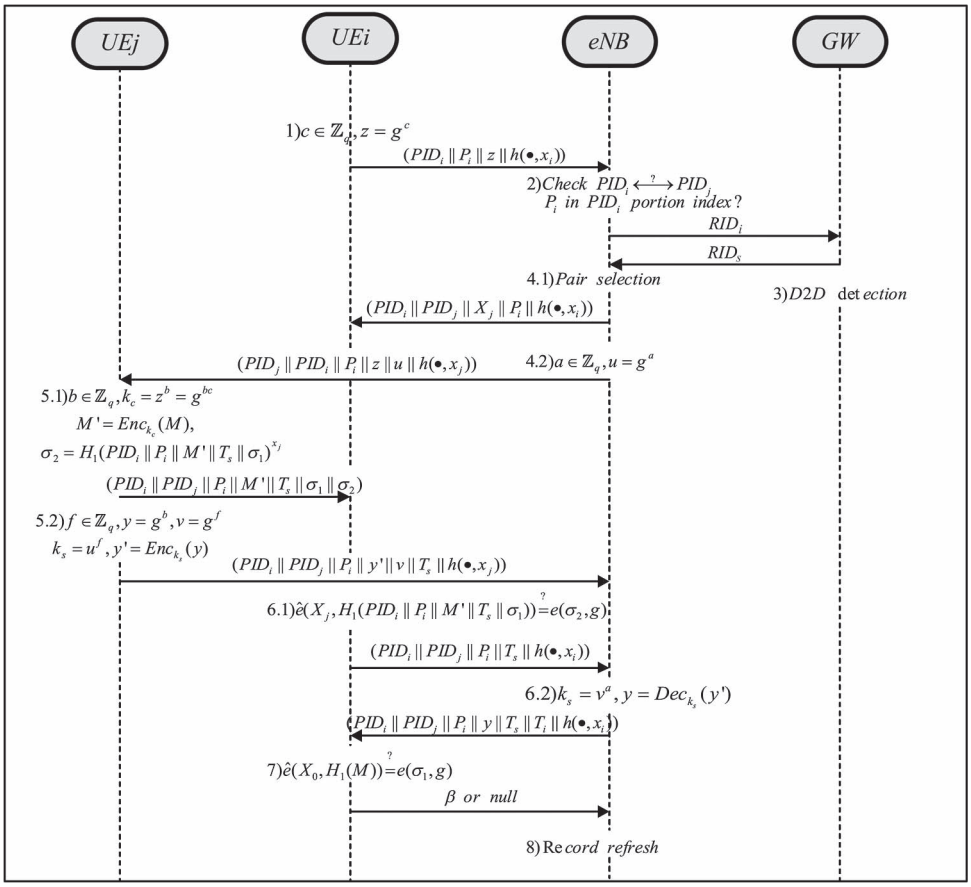

Fig. 2. Secure data sharing protocol.

TABLE V
DATA FORMAT DURING TRANSMISSION

PID_i	PID_j	Portin index (P_i)	$Enc(M)$ (M')	Timestamp (T_s)	Signature (σ_1)	Signature (σ_2)
2 Bytes	2 Bytes	2 Bytes	L Bytes	2 Bytes	20 Bytes	20 Bytes

Step 4 Pair Selection: The eNB chooses the proper candidate (supposing UE_j), the portion index of which meets with the demand, as the server. Generally, for the balance of load and fairness, the device holding the minus share frequency is selected to act as the transmitter. Then, the eNB randomly selects $a \in \mathbb{Z}_q^*$ and computes $u = g^a$ as a key hint. The communication request message $(\text{PID}_j \| \text{PID}_i \| z \| u \| P_i \| h(\bullet, x_j))$ is then sent to the selected entity. Simultaneously, the eNB acknowledges the requesting UE the pseudoidentity PID_j and public key X_j of the transmitter, which means $(\text{PID}_i \| \text{PID}_j \| X_j \| P_i \| h(\bullet, x_i))$ being sent to UE_i as a response.

Step 5 Data Transmission: When receiving a communication request message

$$\text{PID}_j \| \text{PID}_i \| z \| u \| P_i \| h(\bullet, x_i)$$

the entity randomly selects $b \in \mathbb{Z}_q^*$ and generates the communication key $k_c = z^b = g^{cb}$. With k_c, the entity encrypts the material M and gets $M' = \text{Enc}_{k_c}(M)$. Before sending the secure message M, the entity signs the message by computing

$$\sigma_2 = H_1(\text{PID}_j \| P_i \| M' \| T_s \| \sigma_1)^{x_j}. \tag{3}$$

The data is shaped in the format of Table V and sent to the intended UE. Note that signature σ_1 is finished in the offline stage by the SP. Timestamp T_s is applied to resist the replay attack.

Additionally, the key hint $y = g^b$ is computed for the receiver to generate the decryption key k_c. Rather than being sent to the receiver directly, the key hint is encrypted under the shared key k_s with eNB, where $k_s = u^f$, $f \in \mathbb{Z}_q^*$, and $v = g^f$. Thus, the transmitter sends a report $(\text{PID}_i \| \text{PID}_j \| P_i \| \| \text{Enc}_{k_s}(y) \| v \| T_s \| h(\bullet, x_j))$ to the eNB for the data sharing event so that its shared frequency record can be refreshed.

Step 6 Entity Verification: Once a packet is received, UE_i extracts PID_j from the message. It compares PID_j with the pseudoidentity obtained from the eNB. If they do not match, the packet is dropped. Otherwise, it performs signature verification by checking, i.e.,

$$\hat{e}\left(X_j, H_1(\text{PID}_j \| P_i \| M' \| T_s \| \sigma_1)\right) \overset{?}{=} \hat{e}(\sigma_2, g). \tag{4}$$

If the equation holds, the data are considered sent by the entity with pseudoidentity PID_j. To decrypt the message M', UE_i sends a key hint request message $(\text{PID}_i \| \text{PID}_j \| P_i \| T_s \| h(\bullet, x_i))$ to the eNB.

As the key hint requests message arrives, the eNB first checks if the time information of the message is in the time

allowable window. If so, it decrypts the $\mathrm{Enc}_{k_s}(y)$ with $k_s = v^a$ and a response, i.e.,$(\mathrm{PID}_i \| \mathrm{PID}_j \| P_i \| \| y \| T_s \| T_i \| h(\bullet, x_i))$, is delivered. Timestamp T_i is employed to record the feedback time, which is later analyzed in Step 8.

Step 7 Data Verification: With the reception of key hint y, UE_i can get the communication key by computing $k_c = y^c = g^{bc}$. Thus, the payload M' is decrypted, and the original material M is revealed. To ensure the authority of the data, the signature is verified by checking the following:

$$\hat{e}\left(X_0, H_1(P_i \| M)\right) \stackrel{?}{=} \hat{e}(\sigma_1, g). \tag{5}$$

If the equation holds, the data are accepted. Otherwise, it is considered that the impersonation attack may have occurred. Then UE_i is assumed to report a beacon, i.e.,

$$\beta = (\mathrm{PID}_i \| \mathrm{PID}_j \| P_i \| \| M' \| T_s \| \sigma_1 \| \sigma_2 \| h(\bullet, x_i))$$

to the eNB within the timestamp T_i', which satisfies that $T_i' < T_i + \Delta T$ (ΔT is the predefined time scale). The feedback beacon β, acting as the evidence of the fake message, is employed to track the malicious attacker, which is analyzed in Section V.

Step 8 Record Refresh: The eNB waits for ΔT after sending the key hint response to UE_i. During the waiting time scale, if any feedback beacon arrives, the eNB first checks the validity of σ_1 by inspecting (5) as UE_i had implemented. Note the payload M is not obtained by deciphering M' as the eNB knows no information about the communication key k_c. Instead, it refers to the storage for the original data M with the corresponding portion index. If the signature σ_1 is invalid indeed, it is judged that the message did not originate from the SP and may be fabricated by the adversary. Then, the record in eNB is refreshed by the following stages.

1) The eNB verifies the validity of signature σ_2 to ensure that the fake message is sent by the entity with pseudoidentity PID_j.
2) The eNB refers to record Table III to disclose the RID of PID_j.
3) The malicious behavior amount record of the corresponding entity adds one.

Note that punishment will be taken against the violators if the record of malicious behaviors reaches a certain level. Accordingly, the frequency that the beacon is sent to the eNB is not that large, and it will not consume too much upstream bandwidth.

If no feedback beacon appears during the waiting time scale or the signature σ_1 is valid, the record table is refreshed by the following stages.

1) P_i is inserted in the portion index item of PID_i.
2) The shared frequency of PID_j adds one.

C. Availability Analysis

At the initial phase of the system establishment, only the SP owns the data, which is supposed to be sent to all the legitimate members of the system. Consider the case that all the members, maybe as many as hundreds, send service requests to the eNB simultaneously while only one SP is available. Bottleneck does not lie in the authentication ability of the eNB and the detection time of the GW due to their strong capability but in the serious lack of enough SP candidates. Therefore, the performance is assumed enhanced by assigning more SPs in the spot. However, this approach will increase the cost of operators. Accordingly, it is recommended in our protocol that, at the system setup stage, some of the UE registers are selected to be equipped with the original material and the signature of the SP. Then, they perform as the proxy SPs and play the role of the authentic SP. It is worth noting that, in order to avoid interference between D2D links, power control and interference management are implemented in D2D communications [7].

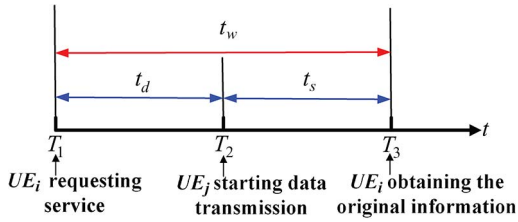

Fig. 3. Time periods of the data sharing process.

Since the processes of establishing proxy SPs are time-consuming, it is a challenging issue to determine how many proxy SPs are moderate for a tradeoff between the cost and availability. The amount depends on the demanding performance. To clarify this point, we plot Fig. 3 and give definitions on the time periods of the protocol.

Definition 2: Delay t_d. Delay is defined as the time period from the UE sending a service request to the transmitter starting to transmit the information.

Definition 3: Service time t_s. Service time is defined as the time period from the transmitter starting to transmit the information to the receiver obtaining the demanded information.

Definition 4: Waiting time t_w. Waiting time is defined as the period from the UE sending a service request to obtaining the demanded information. Evidently, $t_w = t_d + t_s$.

Definition 5: $(N, t_s, \Delta t)$-availability. A system is $(N, t_s, \Delta t)$-availability if the average delay for the N members to get service is less than Δt with average service time t_s.

Let the UE requesting service event be a Poisson process with arriving rate λ, and t_r be the interarrival time for a user requesting message. Then, t_r has an exponential distribution with mean $1/\lambda$. The relationship between the average interarrival time of the user and the average service time may vary in different application scenarios. In *Case 1*, i.e., $(1/\lambda) \ll t_s$, the users may send service request messages simultaneously (the specific relationship between $1/\lambda$ and t_s will be analyzed later) to the eNB (e.g., in the concert scenario, all the users want to obtain the information when the concert finished). In *Case 2*, i.e., $(1/\lambda) > t_s$, the users requesting services may arrive at a larger time interval than the service time. In *Case 3*, the arriving rate of the users may be between *Case 1* and *Case 2*.

Given *Definition 5*, to guarantee $(N, t_s, \Delta t)$-availability, we get average delay $t_d < \Delta t$, whereas the delay varies in different cases, which is analyzed in the following lemmas. Meanwhile, the lemmas investigate the relationship between the number of the proxy SPs and delay.

TABLE VI
INFECTED DEVICES INCREASE WITH TIME

Timestamp	0	t_s	$2t_s$	$3t_s$	$\cdots$	nt_s
Infected devices	m	$2m$	$4m$	$8m$	$\cdots$	N

Lemma 1: In Case 1, the number of proxy SPs in the SeDS protocol is m for providing the system with $(N, t_s, \Delta t)$-availability, where m satisfies the following:

$$t_d = \frac{N \times (n-1) - (2^n - 2) \times m}{N - m} t_s \leq \Delta t \tag{6}$$

where $n = \lfloor \log_2(N/m) \rfloor$.

Proof: In *Case 1*, the average interarrival time is much less than the service time; thus, it is reasonable to assume that all the infected devices, which have obtained the data, transmit message to other peers simultaneously. It can be derived that the number of the infected devices increases at the rate of $2's$ power. Specifically, if there are m infected devices at time T_0, then there will be $2m$ infected devices at time $T_0 + t_s$. Suppose that each information portion is of the same length, which causes the service time of every device being the fixed value t_s. The process is listed in Table VI.

The average delay for N members is

$$\begin{aligned} t_d &= [m \times 0 + 2m \times t_s + 4m \times 2t_s + \cdots + 2^{n-2}m \\ &\quad \times (n-2)t_s + (N - 2^{n-1}m) \times (n-1)t_s]/(N-m) \\ &= \frac{N \times (n-1) - (2^n - 2)m}{N - m} t_s. \end{aligned} \tag{7}$$

Given the *Definition 5*, we get $t_d < \Delta t$, which is $((N \times (n-1) - (2^n - 2) \times m)/(N-m))t_s \leq \Delta t$. ■

Equation (6) does not show the relationship between m and $(N, t_s, \Delta t)$ directly, whereas the simulation results in Section VI-C will give the impact of m on delay distinctly.

Next, we analyze the specific relationship between $1/\lambda$ and t_s rather than the general condition $(1/\lambda) \ll t_s$. From the analysis above, we find out that, as long as the number of the waiting users is larger than the SPs, (7) is established. Through Table VI, we get that the average appearance rate of the infected devices, which serve as the SPs, is N/nt_s. To leave a few redundancies, we consider the requesting rate $\lambda > (Nm/nt_s)$ as the event happens simultaneously. Therefore, $(1/\lambda) < (nt_s/Nm)$ is used to describe the condition $(1/\lambda) \ll t_s$.

Lemma 2: In Case 2, the minimal number of SPs does not influence much on the average delay for the users to share the data.

Proof: Since the interarrival time of requesters is larger than the service time, one SP is enough to provide the service as the service request message arrives after the former one, which has been finished to free up the SP. Therefore, the number of proxy SPs does not influence much on the average delay. ■

From *lemma 2* we conclude that it is not necessary to set proxy SPs if the arriving rate of the service request message is low enough. (The upper limit of the arriving rate will be discussed in Section VI-C in detail.)

Lemma 3: In Case 3, the number of proxy SPs is m for providing the system with $(N, t_s, \Delta t)$-availability, where m satisfies the following:

$$t_d = t_s \left(1 + \frac{m}{N}\right) \ln \left(1 + \frac{N}{m}\right) - t_s - \frac{N}{2\lambda} \leq \Delta t \tag{8}$$

where λ is the average user requesting rate.

In *Case 3*, the average interarrival time of the user is shorter than the service time but is not short enough to be considered requesting the services at the same time as in *Case 1*. This process is proposed by using a queuing model in [30], where the users are considered the customers and where the SPs serve as the servers.

Proof: See the Appendix. ■

Further Discussion: From the Appendix, we get the average delay

$$t_d = t_s \left(1 + \frac{m}{N}\right) \ln \left(1 + \frac{N}{m}\right) - t_s - \frac{N}{2\lambda}. \tag{9}$$

By considering $\rho = m/N$ as the ratio of the proxy SPs to the total arrivals and combining with $t_1 = N/\lambda$ as is analyzed above, (9) is transformed into

$$t_d = t_s(1+\rho) \ln \left(1 + \frac{1}{\rho}\right) - t_s - \frac{t_1}{2}. \tag{10}$$

In terms of (10), it is clear that the average delay for the user is mainly related to the ratio ρ rather than m or N separately. Naturally, the delay is also affected by the service time and the continual time of the arrival event. The results will be evaluated in Section VI-C.

V. SECURITY ANALYSIS

Here, we analyze the security properties of the proposed SeDS protocol following the predefined system model. We will show how the scheme can effectively mitigate the potential threats and meet with the security requirements presented in Section III.

Proposed Protocol Ensures Data Confidentiality and Integrity: During the process of transmission, the data are done with proper encryption $(\text{Enc}_s(M))$. Without gaining the key, the eavesdroppers cannot decrypt the cipher text. However, the key is only shared between the sender and the receiver. Even the receiver, who owns one key hint, is not able to access the original information M before getting the other key hint from the eNB. As for the eavesdropper, who may get both key hints g^b and g^c, it still cannot derive the shared key g^{bc} under the DLP assumption since it has no information about b or c. Thus, the eavesdropping attacks are resisted, and the data confidentiality is guaranteed. Furthermore, in order to resist *man-in-the-middle attack*, HMAC is introduced to provide message integrity and message authentication.

Meanwhile the data correctness and authority are protected by signature σ_1. From the message format Table V, it can be found out that the original information M had been signed by the SP during the transmission. Therefore, with the verification of signature σ_1, the origin of the data is expected to be from SP, being considered the authority SP. Hence, the data integrity and authority are guaranteed.

Proposed Protocol Ensures Entity Authentication: Entity authentication is implemented between the UE and eNB and between the UEs. When UE and eNB exchange information with

each other, the entity authentication is performed by the normal cellular communication. Additionally, the eNB authenticates the membership by checking whether the RID corresponds with the pseudoidentity in the member record Table III.

Generally, the authentication in D2D communication mode is implemented by the verification of the signature σ_2. Before sending the data to another device, the transmitter is assumed to make a signature on its pseudoidentity and the data, as shown in (3). Thus, the receiver can verify the signature to authenticate the pseudoidentity of the sender.

Proposed Protocol is Secure in Conditional Privacy Preservation: In the SeDS protocol, devices use pseudoidentity, which is the secure one-way hash value of the RID, for communication. It is computationally hard to identify the real identity of the entity. Note that the RID of the UE or SP is disclosed to the trust authority eNB, although anonymous to the other devices. Thus, the privacy preservation property is conditional.

The Proposed Protocol is Resistant to Free-Riding Attacks: Free-riding attacks are taken against technically by keeping a record table in the eNB and refreshed after every data transmission event. By referring to the item share frequency in the table, it is easy to find out the member who puts in least effort on sharing data with others. These free-riders may be punished by being not delivered information further more or excluded from the membership.

Proposed Protocol Ensures Nonrepudiation: The data sharing event is nonrepudiation for both the sender and receiver. The signature σ_2 of the transmitter provides no opportunity for the entity to deny the transmitting event, although it also offers the evidence of data sharing behavior, which may be proofed to be meritorious or malicious by the verification of signature σ_1. When a receiver verifies an invalid signature σ_1, it will send a feedback beacon β to the eNB.[8] By verifying the signature σ_1 from the evidence, the eNB first ensures that the message is indeed sent by the entity with pseudoidentity PID_j. Then, by referring to the record table, the RID of the sender is tracked.

Meanwhile, for the decryption of message, the receiver has to send a key hint request message to the eNB. Thus, the reception of the message is discovered. However, there may be irrational attacker who only receives data but does not intend to get the original information; therefore, it will not send a key hint request. In this case, the eNB gets no signal for refreshing the record, which results in the transmitter becoming the victim who does share the data but the eNB has no idea about increasing its share frequency. One solution to this problem might introduce reputation mechanism into the system, which is an open issue.

Proposed Protocol Ensures System Availability: In the defined system, the availability of the service is largely influenced by the delay, the number of the UEs, and the cooperation degree of the UEs.

In the proposed protocol, strategies are adopted to promote the cooperation between the UEs. As is analyzed in the aforementioned security properties, free-riders are detected and punished, which causes the UEs to be active in sharing data with others. Moreover, a nonrepudiation objective obliges the members to act cooperatively during the processes of data transmission.

To ensure the availability of the system, the delay for services should be acceptable by the users. With the performance analysis and evaluation of availability in Section IV-B and C, it can be concluded that the proposed SeDS protocol is expected to provide available service to the users.

VI. Performance Evaluation

Here, we evaluate the performances of the proposed protocol SeDS in terms of computational overhead, communication overhead, and availability in a practical D2D communication environment.

A. Simulation Setting

As the proposed SeDS protocol serves as the first secure data sharing strategy in D2D communication system until this end, we resort to compare the protocol with the data downloading mechanism in [20] because 1) it has the most similar design goals with ours, and 2) it also employs both short group signature (PKI base encryption) and broadcast encryption (symmetric encryption), which are also adopted in our scheme. For the effectiveness and unified measurement of the comparisons, we propose to apply the secure data downloading of [20] in the D2D network architecture directly, namely, SeCD as a benchmark. In SeCD, the *Request Phase* completes the tasks from *Step 1* to *Step 4* of SeDS and *Downloading Phase* performs data transmission and authentication. Meanwhile, the *Downloading vehicles* of SeCD play the role of proxy SPs in SeDS. Note that the biggest differences between SeDS and SeCD lie in two aspects, i.e., the generation of signature and symmetric key. Specifically, SeCD adopts short group signature scheme [22] and broadcast encryption [20], resulting in different performances with SeDS.

A total of $N \geq 2$ users equipped with communication radius of 250 m are randomly deployed in an interested area of 500 m $\times$ 500 m. To depict a realistic scenario for data transmission over a D2D link underlaying LTE-A network, the communication rate may reach 100 Mb/s [31], which causes 0.08-μs transmission delay for per byte message, and the CPU processing speed is set to be 1 GHz as in most current intelligent mobile terminals. Meanwhile, for a typical 80-bit security level, the system parameters k and q are 80 and 160 bits, separately, and Advanced Encryption Standard (AES) serves as the symmetric encryption algorithm. Additionally, we set the number of domains $A = 1$, the members $B = N$, and the probability of users from foreign domains $q_a = 0$ in SeCD.

B. Computational and Communication Overhead

Computational Overhead: Since the pairing and multiplication computation and encryption operation dominate the computational overhead, we consider only these operations in the following estimation. In [32], the implementation is executed on an Intel Pentium 3.0-GHz processor for an MNT curve of embedding degree $= 6$ and 160-bit q. The measured processing

[8]The receiver is stimulated to send the beacon; otherwise, the eNB will refresh the record by inserting the P_i in its portion index item, which will stop the eNB from responding to the P_ith data service request from it.

TABLE VII
EXECUTION TIME FOR DIFFERENT OPERATIONS

Notations	Description	Execution time (ms)
t_p	Time for one pairing	13.5
t_n	Time for one exponential computation	1.8
t_e	Time for one symmetric encryption of L bytes data	$2.8L \times 10^{-5}$

time is 4.5 ms for one pairing operation and 0.6 ms for one multiplication in $\mathbb{G}$. Thereafter, the computation of pairing and point multiplication with similar parameters as ours on a 1-GHz microprocessor can be roughly estimated as $(4.5 \times 3)/1 = 13.5$ ms and $(0.6 \times 3)/1 = 1.8$ ms separately. It is reported in [17] that the processor takes 0.984 μs for AES to encrypt 64-B data on a 1.8-GHz laptop PC; thus, it takes $0.984 \times 1.8 = 1.771$ μs on a 1 GHz microprocessor. Then, it takes $(1.771/64)L = 0.028L$ μs to encrypt an L-byte data, which is shown in Table VII.

In the proposed SeDS protocol, formatting the data in *Step 5* requires two exponential computations and an encryption operation, which introduces $2t_n + t_e$ time cost. To authenticate the validity of signature σ_1 and σ_2, $4t_p$ are needed, as shown in Fig. 2. Therefore, the total computational overhead of the user is $4t_p + 2t_n + t_e$ time cost. Apart from the user's computation operation, the eNB also performs computation for the decryption of the key hint sent from the transmitter candidate, which yields $2t'_n + t'_e$ time cost, where t'_n and t'_e are time cost in eNB for one exponential computation and decryption, separately.[9] In SeCD, $14t_p + 38t_n + t_e$ time cost is demanded according to [22].

Communication Overhead: In SeDS, the communication overhead between the UE and eNB for service request and response is $44 + 46 = 90$ B, where the first term represents the overhead caused by the requesting message from the UE, and the second term represents the length of the response message sent by the eNB. Due to the D2D candidate detection process, the communication overhead between the eNB and GW is $2 + 2n_c$, where n_c is the number of the candidate detected by GW. To inform the selected candidate to share data, the eNB is supposed to send a message causing 66-B overhead, as shown in 4.2 of Fig. 2. The communication overhead generated by the device-to-device data sharing is $L + 48$ B, according to Table V. Finally, for the decryption of the data, additional $68 + 28 + 50 = 146$ B of key hint is transmitted between the UE and eNB.[10] In SeCD, the request phase produces 2+192-B communication overhead, whereas during the data downloading phase $L + 196 +$ 66-B data are transmitted. The computational and communication overhead comparisons between SeDS and SeCD are listed in Table VIII.

Remark 3: The overhead at the transmission layer, network layer, and link layer may also increase in SeDS. As the overhead of application message dominates the communication overhead in most cases [22], we only consider the application layer overhead for simplification.

[9]The eNB may decrypt the key hint beforehand to reduce the delay when it is asked to transmit it.

[10]The communication overhead for the eNB is $304 + 2n_c$ B. As a result, our protocol achieves security goals at the cost of bringing acceptable implementation complexity to the eNB. Due to the fact that the eNB is scalable and flexible, we think it is worth it to realize data security by increasing complexity to eNB at some level.

TABLE VIII
OVERHEAD COMPARISONS BETWEEN SEDS AND SECD

Overhead	SeDS	SeCD
Computational overhead	$4t_p + 2t_n + t_e$	$14t_p + 38t_n + t_e$
Communication overhead	$L + 186 + 2n_c$	$L + 458 + 2n_c$

C. Availability Evaluation

In the following, we evaluate the availability in detail. First, we analyze the components of service time t_s.

In the proposed SeDS protocol, before starting to get the information from the transmitter, the UE has to wait for the authentication of the eNB and candidate detection of GW, represented by t_m. Based on the given analysis, the time t_m is occupied by the message transmission delay between the entities, where

$$\begin{aligned} t_m &= (90 + 2 + 2n_c + 66) \times 0.08 \\ &= (12.64 + 0.16n_c)\ \mu\text{s} \end{aligned}$$

in which n_c is less than the number of the UEs distributed in the scenario. After the data transmission process has been finished, the UE has to perform several computational operations to access the original information, as is explored in Section VI-B. Thus, the data access time

$$\begin{aligned} t_a &= (L + 48 + 146) \times 0.08 \times 10^{-3} + 4t_p + 2t_n + t_e \\ &= 1.08L \times 10^{-4} + 106\ \text{ms} \end{aligned}$$

which is much larger than t_m. Accordingly, t_m is negligible compared with the data access time. Thus, the service time $t_s = t_m + t_a \cong t_a$. With the same analysis processes in SeCD, the service time $t_s = 1.08L \times 10^{-4} + 257$ ms.

As indicated in Section IV-C, the delay estimation model is different with user requesting rate varying. Hence, it is necessary to bound the user requesting rate and to evaluate the average delay.

1) User Requesting Bound: In *Case 1*, $(1/\lambda) < (nt_s/Nm)$. Then, we get

$$\lambda > \frac{m \times N}{n \times t_s} \triangleq \lambda_l \tag{11}$$

where $n = \lfloor \log_2(N/m) \rfloor$, and λ_l represents the user requesting rate low bound in *Case 1*.

Fig. 4(a) shows the simulation results. It is found out that, with the increase in m, the low bound rises up almost linearly, which indicates that slightly adding SPs at the initial stage may improve the system capacity efficiently. Note that there exist some special points at which the rate goes up suddenly, e.g., $m = 6$ and $m = 7$ when $N = 200$. This is because when $m = 6$ and $m = 7$ separately, $n = \lfloor \log_2(N/m) \rfloor$ varies from 5 to 4, which causes jump at these points.

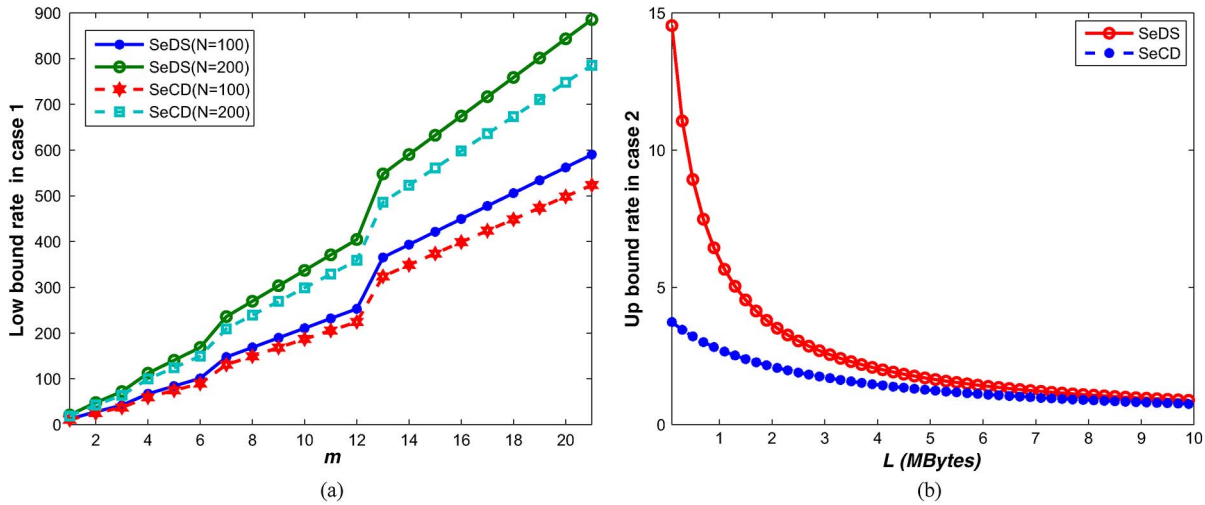

Fig. 4. User requesting rate. (a) Lower bound varies with the minimal initial SPs in *Case 1*. (b) Upper bound varies with data length in *Case 2*. (a) $L = 10$ MB. (b) $N = 100$.

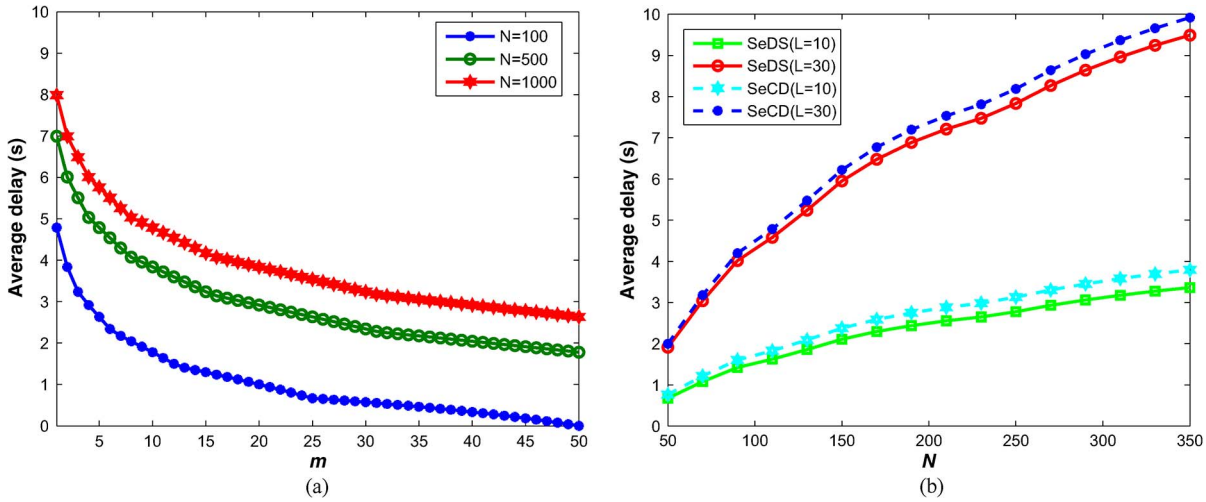

Fig. 5. Average delay varies with (a) the minimal initial SPs and (b) the number of UEs in *Case 1*. (a) $t_s = 1$ s. (b) $m = 15$.

In *Case 2*, when $(1/\lambda) > t_s$, the users may not have to wait for service under the condition

$$\lambda < \frac{1}{t_s} \triangleq \lambda_u \tag{12}$$

where λ_u represents the user requesting rate upper bound. Intuitively, an increase in date length may descend the upper bound in *Case 2*. To better understand, the degree to which the effect of L on λ_u, we illustrate this issue by simulating (12) and get Fig. 4(b), in which the result is explained in detail. From the figure, we discover that the upper bound may go below one when the data length arrives 10 MB in both SeDS and SeCD protocols. This result shows that the arrival rate should not exceed one every second when the data length is larger than 10 MB. Therefore, we conclude that the achievement is perfect in *Case 2*, but the prerequisite is harsh. Fig. 4(a) and (b) indicate that the bound of SeDS is slightly higher than the corresponding bound of SeCD, due to the longer service time in SeCD for the same material. However, with L increasing, the bounds become closer because the service time is dominated by the value of L, and the time differences are shortened by larger L.

2) Average Delay in Case 1: Equation (6) gives computation method for average delay t_d in *Case 1*. To investigate the relationship between t_d and other parameters, we study the relationship between t_d and m in Fig. 5(a) and N in Fig, 5(b). The results imply that increasing the number of SPs will definitely reduce the delay, which may reach as low as zero if m is half of the number of the users, e.g., $m = 50$ when $N = 100$, as shown in Fig. 5(a). However, it is not practical to predistribute so many SPs due to high cost. Generally, it is necessary to select a moderate m to trade off the cost and average delay so that the availability demand is satisfied. Meanwhile, Fig. 5(b) demonstrates the impact of N on the average delay, which may go up as the number of users increases, although the ascendant trend is different as the service time varies. By checking up the figure carefully, it is revealed that the average delay becomes increasingly longer as L increases. The reason is the waiters have to waste more time until the formers obtain services. This result may instruct the operators to divide long contents

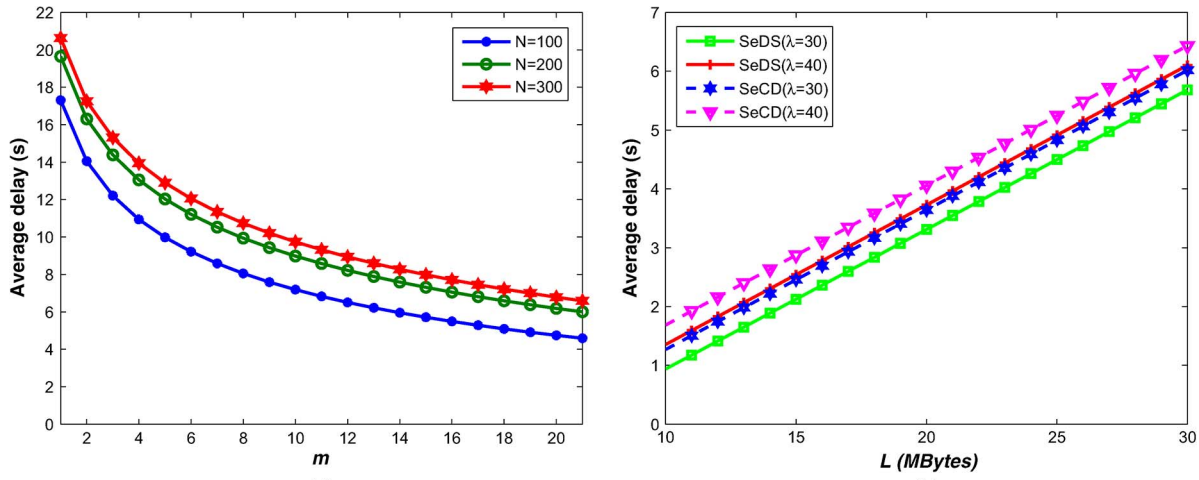

Fig. 6. Average delay varies with (a) the minimal initial SPs and (b) the data length in Case 3. (a) $t_s = 5$ s , $\lambda = 50$. (b) $N = 100$, $m = 15$.

into proper frames to guarantee system availability. It is also revealed in Fig. 5(b) that the average delay in SeDS is smaller than that in SeCD, demonstrating the availability of our proposed protocol. Note that the distances between SeDS and SeCD increase with N rising up, which displays the advantages of the proposed SeDS in a large-scale system.

3) Average Delay in Case 3: The queuing model of *Case 3* makes the computation of average delay a little complicated. Simulation results are shown in Fig. 6, which indicates that the average delay varies with the number of proxy SPs and data length. As expected, the average delay decreases with the increase in m, whereas on the opposite, it ascends linearly with the increase in L. It is worth noting that, in Fig. 6(a) and (b), different lines are not far apart from each other, which means that the number of N and arrival rate λ do not affect the average delay in *Case 3* much. This is due to the fact that, when the arrival rate is moderate as in *Case 3*, the average delay is mainly determined by m and t_s, although slightly influenced by N and λ. Therefore, it makes sense to enhance SPs at initial stages or curtail service time for the improvement of availability in *Case 3*. Meanwhile, we find in Fig. 6(b) that the average delay in SeDS at $\lambda = 40$ and SeCD at $\lambda = 30$ are of the same level, which verifies that the proposed protocol has higher throughput than that of the benchmark.

To further research the relationship between the variables, additional experiments are finished to explore how average delay varies with the ratio of m to N in *Case 3*. As shown in Fig. 7, increasing the ratio will efficiently reduce the delay, particularly when the service time is long. Nevertheless, when the ratio is high enough (e.g., 0.36 at $L = 50$ MB), further increasing the ratio may not lead to advantageous improvement. Additionally, from the figure, we find that as ρ goes up, the average delay differences between SeDS and SeCD become smaller, which shows that our proposed SeDS scheme has superiority when the ratio of m to N is small.

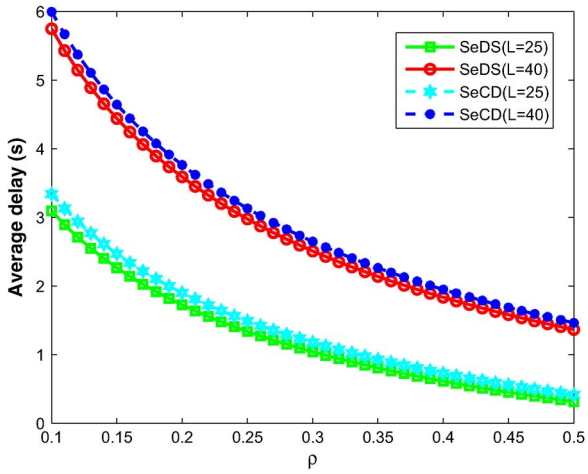

Fig. 7. Average delay varies with the ratio of m to N (the continual time of the arrival event $N/\lambda = 2$).

VII. Conclusion

We have proposed a secure data sharing protocol (SeDS) for D2D communication in an LTE-A network. By considering the features and security requirements of the system, the protocol is elaborately designed to achieve the desired objectives without causing extra load to the cellular networks. In particular, based on digital signature and symmetric encryption, the proposed protocol satisfies security goals in terms of data confidentiality and integrity, transmission and reception nonrepudiation, entity authentication, and free-riding resistant. Moreover, the availability target is emphasized by establishing delay evaluation models to investigate the impacts of proxy SPs on delay in different application scenarios. To the best of our knowledge, the proposed protocol is the first study on secure data-sharing strategy in D2D communication; thus, the work sheds light on this research line. It should be noted that the limitation of this paper lies in the assumption that the communication between the eNB and GW is secure, although in hostile environment, the channel might be compromised.

For the future work, we will consider secure data sharing between devices without the involvement of eNB and GW; thus, completely offloading the cellular network and cooperation is expected to be explored in D2D communications. Meanwhile, we will extend this work by studying a more general and

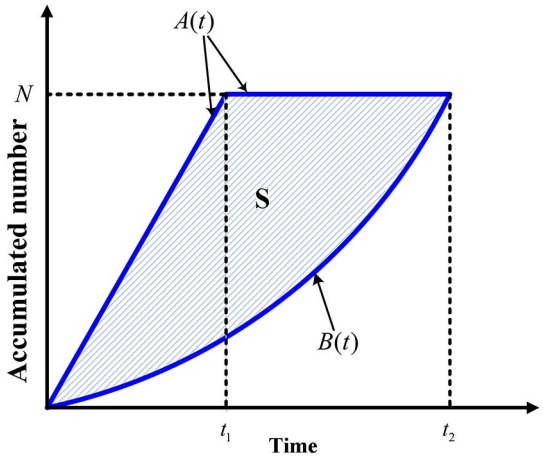

Fig. 8. Accumulated number and the delay.

complicated application scenario in which the service time is not deterministic, and we will exploit the effects of mobility on security in D2D communication.

APPENDIX
PROOF OF LEMMA 3

According to queuing theory, our system is presented in the form of $M/D/n$, where we have the following.

- M represents the interarrival time for exponential distribution.
- D represents service time for deterministic distribution.
- n represents the number of servers.

To discuss the influence of the proxy SPs on the average delay, we plot Fig. 8 for clarification of this issue. We assume that the arrival event and service is consecutive. In Fig. 8, $A(t)$ describes the accumulated arrivals before time t, whereas $B(t)$ represents the accumulated departures. The shadow area S displays the total delay, and we can get the average delay $t_d = S/N$, where N is the total number of arrivals of the system. In our proposed system, the users arrive according to a Poisson process with rate λ and stop joining when all the N members arrive; thus

$$A(t) = \begin{cases} \lambda t, & t \le t_1 \\ N, & t > t_1 \end{cases} \tag{A1}$$

where $t_1 = N/\lambda$. Note that, in the D2D service model, the number of the servers increases with time as the devices that have been served perform as servers next time, i.e., the departures become the servers. Thus, we get

$$\frac{dB(t)}{dt} = (B(t) + m)\,\mu \tag{A2}$$

where

- $dB(t)/dt$ represents the service rate at time t;
- μ is the service rate of every SP;
- $B(t) + m$ is the number of SPs at time t.

By solving (A2) with $B(0) = 0$ and $(dB(t)/dt)|_{t=0} = m\mu$, we obtain

$$B(t) = me^{\mu t} - m \tag{A3}$$

where $\mu = 1/t_s$. Then

$$S = \frac{1}{2}Nt_1 + N(t_2 - t_1) - \int_0^{t_2} B(t)dt \tag{A4}$$

where t_2 represents the time when the last arrived user is served, which indicates $B(t_2) = N$. Thereby, we get $t_2 = \ln((N + m)/m)/\mu$.

Combining (A2)–(A4), we get

$$S = \frac{N+m}{\mu}\ln\left(1 + \frac{N}{m}\right) - \frac{N^2}{2\lambda} - \frac{N}{\mu} \tag{A5}$$

$$t_d = \frac{S}{N} = t_s\left(1 + \frac{m}{N}\right)\ln\left(1 + \frac{N}{m}\right) - \frac{N}{2\lambda} - t_s. \tag{A6}$$

Given *Definition 5*, we get $t_d < \Delta t$, which is $t_s(1 + (m/N))\ln(1 + (N/m)) - t_s - (N/2\lambda) \le \Delta t$. ■

REFERENCES

[1] D. Wu, J. Wang, R. Q. Hu, Y. Cai, and L. Zhou, "The role of mobility for D2D communications in LTE-advanced networks: Energy vs. bandwidth efficiency," *IEEE Wireless Commun.*, vol. 21, no. 4, pp. 66–71, Apr. 2014.

[2] M. Yang, S. Y. Lim, H. J. Park, and N. H. Park, "Solving the data overload: Device-to-device bearer control architecture for cellular data offloading," *IEEE Veh. Technol. Mag.*, vol. 8, no. 1, pp. 31–39, Mar. 2013.

[3] L. Zhou, Y. Wen, H. Wang, and M. Guizani, "Resource allocation with incomplete information for QoE-driven multimedia communications," *IEEE Trans. Wireless Commun.*, vol. 12, no. 8, pp. 3733–3745, Aug. 2013.

[4] L. Zhou, R. Hu, Y. Qian, and H.-H. Chen, "Energy-Spectrum efficiency tradeoff for video streaming over mobile ad hoc networks," *IEEE J. Sel. Areas Commun.*, vol. 31, no. 5, pp. 981–991, May 2013.

[5] S. Ryu, S. Park, N. Park, and S. Chung, "Development of device-to-device communication based new mobile proximity multimedia service business models," in *Proc. IEEE Int. Conf. Multimedia Expo Workshops*, pp. 1–6, 2013.

[6] B. Zhou, H. Hu, S. Huang and H. Chen, "Intracluster device-to-device relay algorithm with optimal resource utilization," *IEEE Trans. Veh. Technol.*, vol. 62, no. 5, pp. 2315–2326, Jun. 2013.

[7] H. Min, J. Lee, S. Park, and D. Hong, "Capacity enhancement using an interference limited area for device-to-device uplink underlaying cellular networks," *IEEE Trans. Wireless Commun.*, vol. 10, no. 12, pp. 3995–4000, Dec. 2011.

[8] H. Min, W. Seo, J. Lee, S. Park, and D. Hong, "Reliability improvement using receive mode selection in the device-to-device uplink period underlaying cellular networks," *IEEE Trans. Wireless Commun.*, vol. 10, no. 2, pp. 413–418, Feb. 2011.

[9] L. Zhou, Z. Yang, H. Wang, and M. Guizani, "Impact of execution time on adaptive wireless video scheduling," *IEEE J. Sel. Areas Commun.*, vol. 32, no. 4, pp. 760–772, Apr. 2014.

[10] L. Zhou, Z. Yang, Y. Wen, and J. Rodrigues, "Distributed wireless video scheduling with delayed control information," *IEEE Trans. Circuits Syst. for Video Technol.*, vol. 24, no. 5, pp. 889–901, May. 2014.

[11] L. Zhou, D. Wu, B. Zheng, and M. Guizani, "Joint physical-application layer security for wireless multimedia delivery," *IEEE Commun. Mag.*, vol. 52, no. 3, pp. 66–72, Mar. 2014.

[12] J. Yue, C. Ma, H. Yu, and W. Zhou, "Secrecy-based access control for device-to-device communication underlaying cellular networks," *IEEE Commun. Lett.*, vol. 17, no. 11, pp. 2068–2071, Nov. 2013.

[13] X. Chen, B. Proulx, X. Gong, and J. Zhang, "Social trust and social reciprocity based cooperative D2D communications," in *Proc. ACM Int. Symp. MOBIHOC Netw. Comput.*, Bangalore, India, Jul. 29–Aug. 1, 2013, pp. 187–196.

[14] C. Yu, C. Lu, and S. Kuo, "Noninteractive pairwise key establishment for sensor networks," *IEEE Trans. Inf. Forensics Security*, vol. 5, no. 3, pp. 556–569, Sep. 2010.
[15] R. Lu, X. Lin, and X. Shen, "SPOC: A secure and privacy-preserving opportunistic computing framework for mobile-healthcare emergency," *IEEE Trans. Parallel Distrib. Syst.*, vol. 24, no. 3, pp. 614–624, Mar. 2013.
[16] M. Mana, M. Feham, and B. Bensaber, "Trust key management scheme for wireless body area networks," *Int. J. Netw. Security*, vol. 12, no. 2, pp. 75–83, 2011.
[17] D. He, J. Bu, S. Zhu, S. Chan, and C. Chen, "Distributed access control with privacy support in wireless sensor networks," *IEEE Trans. Wireless Commun.*, vol. 10, no. 10, pp. 3472–3481, Oct. 2011.
[18] X. Lin, R. Lu, X. Shen, Y. Nemoto, and N. Kato, "SAGE: A strong privacy-preserving scheme against global eavesdropping for eHealth systems," *IEEE J. Sel. Areas Commun.*, vol. 27, no. 4, pp. 365–377, May 2009.
[19] X. Liang, X. Li, R. Lu, X. Lin, and X. Shen, "Morality-driven data forwarding with privacy preservation in mobile social network," *IEEE Trans. Veh. Technol.*, vol. 61, no. 7, pp. 3209–3222, Sep. 2012.
[20] Y. Hao, J. Tang, and Y. Cheng, "Secure cooperative data downloading in vehicular ad hoc networks," *IEEE J. Sel. Areas Commun.*, vol. 31, no. 9, pp. 523–537, Sep. 2013.
[21] X. Lin, "LSR: Mitigating zero-day sybil vulnerability in privacy-preserving vehicular peer-to-peer network," *IEEE J. Sel. Areas Commun.*, vol. 31, no. 9, pp. 237–246, Sep. 2013.
[22] X. Lin, X. Sun, P. Ho, and X. Shen, "GSIS: A secure and privacy preserving protocol for vehicular communications," *IEEE Trans. Veh. Technol.*, vol. 56, no. 6, pp. 3442–3456, Nov. 2007.
[23] Y. Park, C. Sur, C. Jung, and K. Rhee, "An efficient anonymous authentication protocol for secure vehicular communications," *J. Inf. Sci. Eng.*, vol. 26, no. 3, pp. 785–800, May 2010.
[24] S. Yu *et al.*, "Discriminating DDoS attacks from flash crowds using flow correlation coefficient," *IEEE Trans. Parallel Distrib. Syst.*, vol. 23, no. 6, pp. 1073–1080, Jun. 2012.
[25] T. Thapngam, S. Yu, W. Zhou, and S. Makki, "Distributed Denial of Service (DDoS) detection by traffic pattern analysis," *Peer-to-Peer Netw. Appl.*, vol. 7, no. 4, pp. 346–358, Dec. 2012.
[26] D. Boneh and M. Franklin, "Identity-based encryption from the Weil pairing," in *Proc. Int. Cryptol. Conf.*, 2001, vol. 2139, LNCS, Springer-Verlag, pp. 213–229.
[27] A. Miyaji, M. Nakabayashi, and S. Takano, "New explicit conditions of elliptic curve traces for FR-reduction," *IEICE Trans. Fundam.*, vol. E84-A, no. 5, pp. 1234–1243, May 2001.
[28] W. Diffie and M. E. Hellman. "New directions in cryptography," *IEEE Trans. Inf. Theory*, vol. IT-22, no. 6, pp. 644–654, Nov. 1976.
[29] C. Paar and J. Pelzl, *Understanding Cryptography—A Textbook for Students and Practitioners*. Berlin, Germany: Springer-Verlag, 2010.
[30] L. Kleincock, *Queuing Systems, Volume: Theory*. New York, NY, USA: Wiley, 1975.
[31] A. Ghosh, R. Ratasuk, B. Mondal, N. Mangalvedhe, and T. Thomas, "LTE-Advanced: Next-generation wireless broadband technology," *IEEE Wireless Commun.*, vol. 17, no. 3, pp. 10–22, Jun. 2010.
[32] M. Scott, Efficient Implementation of Cryptographic Pairings. [Online]. Available: http://www.pairing-conference.org/2007/invited/Scott_slide.pdf

Aiqing Zhang (S'14) received the M.S. degree in circuits and systems from Xiamen University, Xiamen, China, in 2006. She is currently working toward the Ph.D. degree with the Department of Telecommunications and Information Engineering, Nanjing University of Posts and Telecommunications, Nanjing, China.

She is also an Associate Professor with Anhui Normal University, Wuhu, China. Her research interests include wireless network security and device-to-device communications.

Jianxin Chen (M'13) received the Ph.D. degree in electronics engineering from Shanghai Jiaotong University, Shanghai, China, in 2007.

From May 2008 to July of 2009, he was a Postdoctoral Researcher with the IPP Hurray Research Group. From 2009 to 2010, he was as a Researcher in a Spanish research center and a Visiting Scholar with the University of Nebraska–Lincoln, Lincoln, NE, USA. He is currently an Associate Professor with the School of Information and Telecommunication Engineering, Nanjing University of Posts and Telecommunications, Nanjing, China. His research interests include body sensor networks and e-health.

Rose Qingyang Hu (S'95–M'98–SM'06) received the B.S. degree in electrical engineering from the University of Science and Technology of China, Hefei, China; the M.S. degree in mechanical engineering from Polytechnic Institute of New York University, Brooklyn, NY, USA; and the Ph.D. degree in electrical engineering from the University of Kansas, Lawrence, KS, USA.

From January 2002 to June 2004, she was an Assistant Professor with the Department of Electrical and Computer Engineering, Mississippi State University, MS, USA. She has more than ten years of R&D experience with Nortel, Blackberry, and Intel as a Technical Manager, as a Senior Research Scientist, and as a Senior Wireless System Architect. She was Nortel fourth-generation (4G) system-level simulation prime and led Nortel 4G standards and technology performance evaluation. She is currently an Associate Professor with the Department of Electrical and Computer Engineering, Utah State University, Logan, UT, USA. She has published extensively and holds numerous patents in her research areas. Her current research interests include next-generation wireless communications, wireless network design and optimization, green radios, multimedia quality of service/quality of experience, communication and information security, wireless system modeling, and performance analysis.

Dr. Hu is currently serving on the editorial boards of IEEE WIRELESS COMMUNICATIONS MAGAZINE, IEEE INTERNET OF THINGS JOURNAL, and IEEE COMMUNICATIONS SURVEYS AND TUTORIALS. She has served as a six-time Guest Editor for IEEE COMMUNICATIONS MAGAZINE, IEEE WIRELESS COMMUNICATIONS MAGAZINE, and IEEE NETWORK MAGAZINE. He received the IEEE Global Communications Conference Best Paper Award in 2012. She is a Distinguished Lecturer of the IEEE Commmunication Society for 2015–2016 and a member of the Phi Kappa Phi and Epsilon Pi Epsilon Honor Societies.

Yi Qian (M'95–SM'07) is currently an Associate Professor with the Department of Electrical and Computer Engineering, University of Nebraska–Lincoln (UNL), Lincoln, NE, USA. Prior to joining UNL, he worked in the telecommunications industry, academia, and the government. Some of his previous professional positions include serving as a Senior Member of scientific staff and a Technical Advisor with Nortel Networks; a Senior Systems Engineer and a Technical Advisor at several start-up companies; an Assistant Professor with the University of Puerto Rico at Mayaguez, Mayaguez, Puerto Rico; and a Senior Researcher with the National Institute of Standards and Technology. He has a successful track record of leading research teams and publishing research results in leading scientific journals and conferences. Several of his recent journal articles on wireless network design and wireless network security are among the most accessed papers in the IEEE Xplore Digital Library. His research interests include information assurance and network security, network design, network modeling, simulation and performance analysis for next-generation wireless networks, wireless ad hoc and sensor networks, vehicular networks, smart grid communication networks, broadband satellite networks, optical networks, high-speed networks, and the Internet.