The ISC Int'l Journal of Information Security
ISeCure

January 2018, Volume 10, Number 1 (pp. 15–27)
http://www.isecure-journal.org

An Incentive-Aware Lightweight Secure Data Sharing Scheme for D2D Communication in 5G Cellular Networks☆

Atefeh Mohseni-Ejiyeh [1,*], Maede Ashouri-Talouki [1], and Mojtaba Mahdavi [1]
[1] *Department of Information Technology Engineering, Faculty of Computer Engineering, University of Isfahan, Isfahan, Iran*

ARTICLE INFO.

Article history:
Received: 19 October 2017
Revised: 10 January 2018
Accepted: 30 January 2018
Published Online: 31 January 2018

Keywords:
D2D Communications, Traffic Offloading, Security, Lightweight, Data Sharing, Incentive.

Abstract

Due to the explosion of smart devices, data traffic over cellular networks has seen an exponential rise in recent years. Device-to-Device(D2D) communication is a promising solution to boost the capacity of cellular networks and alleviate the heavy burden on backhaul links. However, direct wireless connections between devices in D2D communication are vulnerable to certain security threats. In this paper, we propose an incentive-aware lightweight secure data sharing scheme for D2D communication. We have considered the major security challenges of the data sharing scheme, including data confidentiality, integrity, detecting message modification, and preventing the propagation of malformed data. We have also applied the concept of "virtual check" as an incentive mechanism to motivate users' involvement in the process of data sharing. Unlike the previous studies, our proposed protocol is a stateless protocol and does not depend on the user's contextual information. Therefore, it can be used at any time and from anywhere. The security analysis proves that the proposed protocol resists the security attacks and meets the security requirements. The performance evaluation shows that the proposed protocol outperforms the previous works in terms of communication and computation cost. Thus, the proposed protocol is indeed an efficient and practical solution for secure data sharing in D2D communication.

1 Introduction

The fifth generation of cellular networks are called 5G. Mobile data traffic is growing at an extraordinary rate, especially video, which is predicted to comprise 75% of data traffic by arriving the 5G [1]. Video data is transmitted among many services and applications from social networks and video games [2] to public safety services [3]. Given the anticipated growth of mobile traffic in cellular networks by the arrival of 5G, the demand for traffic offloading approaches becomes an inevitable problem for mobile operators. Among the several approaches proposed to address this problem [4], Device-to-Device (D2D) communication appears to be a satisfactory solution [5].

D2D communication refers to direct communication between devices in cellular networks, established either under the control of operators or directly by

☆ This article is an extended version of an ISCISCâĂŹ2017 paper.

* Corresponding author.
Email addresses: atefeh_mohseni@eng.ui.ac.ir (A. Mohseni-Ejiyeh), m.ashouri@eng.ui.ac.ir (M. Ashouri-Talouki), m.mahdavi@eng.ui.ac.ir (M. Mahdavi)

ISSN: 2008-2045

the users [6]; the operator has zero involvement at the user plane side [1]. Inherently, allowing devices to directly connect to one another is associated with certain security and privacy vulnerabilities [7]. Despite the advantages of D2D communication for services such as live video streaming [8] or data sharing, only a few efforts have been made to address the related security and availability challenges. In this paper, we propose a secure data sharing scheme to securely share the intended multimedia content in D2D communication.

D2D communication relies strongly on user cooperation, so a good incentive scheme can prevent free-riding behaviors that harm user's motivation for cooperation [9]. Besides, adopting D2D communication in applications such as data sharing, could turn out to be a win-win situation for both users and operators if a pricing mechanism is considered for users who get involved in data sharing.

In this paper, for the first time, an incentive-aware lightweight secure scheme for data sharing in D2D communication is proposed, to motivate users to securely share their data with each other. During the data sharing phase, a client user requests data downloading with a "virtual check" [10], which is sent to the eNB. It distributes the request to the users around the client user as a proposal. Motivated by virtual checks, those users may accept or reject the proposal, by bidding their intended reward related to cooperation with the eNB. To choose the best candidate, eNB selects the user with the lowest bid and a similar mobility pattern with that of the client user. When the chosen candidate, known as the proxy user, honestly shares its data with the client user, it obtains the digital signature of the virtual check as a proof of successful data sharing. In the data sharing phase, a symmetric encryption algorithm and a message authentication code (MAC) function can resist various attacks.

To summarize, the main contributions of this paper are three-fold,

- We consider the relevant security requirements of data sharing. Our security analysis shows that our scheme can resist various attacks with the minimum computation overhead compared to previous works.
- a novel incentive mechanism is proposed to stimulate cooperation, which utilizes "virtual checks" with the designated verifiable signature to ensure fair and secure cooperation; the proxy user can obtain credit if they successfully share data.
- We consider user mobility to achieve reliability and better performance as well. The proposed protocol is stateless, thus, users can get the service from anywhere. Additionally, users can be slightly mobile [2] during data sharing.

The rest of the paper is organized as follows. We review the literature in Section 2, the system preliminaries of the proposed protocol are explained in Section 3, the proposed secure data sharing protocol is presented in Section 4, its performance and security are analyzed in Section 5 and finally we conclude the paper in Section 6.

2 Related Work

A large number of studies on D2D communications have been reported [6], most of which represent the challenges of interference management, resource allocation or peer discovery [13, 14]. Despite the importance of security issues in D2D communication, only a few works have focused on the topic [15].

A classification provided by Tehrani *et al.* [16] defines four types of D2D communication: (1) device relaying with operator-controlled link establishment (DR-OC); (2) direct D2D communication with operator-controlled link establishment (DC-OC); (3) device relaying with device-controlled link establishment (DR-DC); and (4) direct D2D communication with device-controlled link establishment (DC-DC). The related security works in D2D communications are discussed in the following.

The authors in [17] present a secure data transmission protocol for mobile health systems by exploiting D2D communication in a DR-DC scenario. Data confidentiality, integrity, mutual authentication, and unforgeability are achieved by using a certificateless generalized signcryption scheme (named CLGSC) which works adaptively in each of the signcryption, signature and encryption modes. However, in this scheme, the source node does not receive a delivery report that shows its messages are successfully delivered to the destination. So their scheme is vulnerable to black/gray hole attack introduced in [18]. Moreover, [17] is an application-oriented scheme limited to mobile health applications and the security requirements of data sharing application like resistance to free-riding attack are not considered.

In [19], a secure solution is proposed to connect users via multi-hop communications for emergency services like public safety. In their scheme, D2D communication between users is established either in a DR-OC scenario or DR-DC. In their scheme, each

[1] Generally the term "user plane" refers to the transmission of user's data packet in LTE

[2] They should not leave corresponding eNB until the end of the protocol

intermediate node is supposed to verify the message before relaying it to the next node; so any message modification can be detected. Although the proposed scheme in [19] ensures confidentiality, integrity, and availability, it is better suited to multi-hop communication among proximity services (ProSe) enabled devices.

Zhang *et al.* [20] proposed a secure data sharing scheme, for a DC-OC scenario, which guarantees availability, data confidentiality, and integrity. They use a public key-based cryptography algorithm to achieve user authentication and a MAC for data origin; however, this imposes communication and computation overhead on the users' side. In addition, in their scheme, devices are considered stationary and must register with eNB to obtain their certificate. Therefore, as evident, the scheme is impractical in cases where users are mobile (which happens frequently in mobile networks).

In [21] a secure and lightweight data sharing scheme is proposed which achieves better performance than [20]. The authors apply an EPS-AKA [11] (which is introduced in Sec. III, D) for user authentication and key agreement. Applying the EPS-AKA results in generating two pairs of integrity and confidentiality keys, for users control and data signaling, by both the user and eNB. Then, a symmetric encryption algorithm and a MAC function are applied for data confidentiality and message integrity. Compared to [20], the scheme of [21] is purely symmetric and lightweight and it is compatible with user mobility. However, the works of [21] and [20] depend on the historical user information, such as share frequency and malicious behavior amounts, which are stored at eNB and should be transmitted between eNBs in mobile scenarios, this becomes even a more complicated problem. On the other hand, by running an instance of EPS-AKA per data sharing request in citeramz, HSS would be involved two times for the sender and receiver's authentication, which results in additional overhead on HSS.

Operators should provide a reasonable incentive mechanism for users who participate in D2D communication [9, 16]. In other words, pricing issues [16] have been the subject of many research works. In [22], the authors propose an incentive contract-based mechanism for D2D communications. In their scheme, to offload the traffic from BS for the data which can be locally accessible, Base Station (BS) broadcasts a contract for users who could participate in content sharing; a volunteer user accepts signing the contract with BS. Finally, only in case of successful communication, BS rewards the user according to the contract. However, the authors fail to mention, in detail, how the BS knows about locally accessible data or how the communication ends successfully. In addition, they do not consider the security requirements of data sharing. In [23], an incentive dissemination scheme for DTN networks is proposed. To disseminate the data from the publisher to one or more subscribers, intermediate nodes get rewarded by relaying the packets via the shortest path that reaches more subscribers. By considering the social relationship among users, authors in [24] proposed an incentive data dissemination scheme for D2D communication. They build a social-physical graph model to pair the users exploiting their social trust and mobility direction together. However, they assumed that social trust can motivate users to disseminate data to each other without a payment mechanism. So, the scheme is impractical in cases wherein social trust between adjacent users is lacking.

In addition to adding an incentive-aware mechanism to the proposed scheme in [21], we also remove the need for running EPS-AKA for each data sharing session; accordingly, we derive the secure integrity and confidentiality keys for the user by using the user's session key with eNB which is agreed during the normal cellular communication, after the user attaches the request to the network[11]. Moreover, to support user mobility, we adopt the secure AKA scheme proposed in [25].

In [25], similar to [26] an AKA protocol was proposed to establish a secure connection between D2D users using an EPS-AKA [11] called UAKA. In [25], for the first time, mobility scenarios such as inter-operator and roaming are considered in LTE-A networks. Although the authors claim resilience against cryptographic attacks such as replay and Man-in-the-Middle (MitM), we found that UAKA suffers from MitM attack in the following way. An attacker can obtain the value of the secret MAC key $K_M = R_p \oplus R_k$ by sniffing the secret R_p, transmitted via an open channel between users, and capturing the values of r_1 and $r_2 (R_k = r_1 \oplus r_2)$, transmitted without any cryptographic protection. Therefore, the MitM attacker can violate the security of authentication and key agreement in UAKA. For more details about UAKA please refer to [25]. However, we use the authentication phase of [25] in our scheme, and not the key agreement phase which we show that it has a security vulnerability. It is worth mentioning that, EPS-AKA [29] does not preserve users' privacy, but this problem could be resolved by applying solutions such as [30]-[32]; however, this is beyond the scope of this paper.

In summary, our protocol is the first incentive-aware lightweight secure data sharing protocol that offloads data traffic from the operators, while guaran-

teeing the confidentiality and integrity of the transmitted data between devices and is compatible with geographical mobility.

3 SYSTEM MODEL AND DESIGN GOALS

3.1 System Model

The main LTE-Advanced network entities include UE, eNB, MME, S-GW, P-GW and HSS that participate in managing and securing the access of D2D users to the network. For the purpose of our service, we also consider a Service Provider (SP). Figure 1 illustrates our system model. **UE**: User Equipment which must be authenticated to gain access to his/her intended data via D2D communication. **MME**: Mobility Management Entity is the brain of the Evolved Packet Core (EPC) and is responsible for security procedures such as user authentication (with the help of HSS), idle management and mobility management among others. **HSS**: Home Subscriber Server has a database of subscriber identities and their private keys. To perform UE authentication and generate their authentication vector (AV), it connects to the Authentication Center (AuC).
eNB: Evolved NodeB is a key element in E-UTRAN responsible for controlling radio resources and managing physical layer issues such as interference. **GW**: S-GW is a gateway to E-UTRAN that serves the UEs by routing the incoming and outgoing IP packets. P-GW, on the other hand, is a terminal point of packet data interface to packet data network. Moreover, it is able to run the proximity service control function to detect adjacent users. **SP**: The Service Provider, in our model, is responsible to provide original data to users.

3.2 Security Requirements and Assumptions

The wireless nature of D2D communication, on one hand, and the considered incentive mechanism on the other, are inherently exposed to certain security attacks by the malicious attackers or selfish users. Thus, security is the essential property for our scheme; therefore, the basic security requirements are listed bellow.

3.2.1 Mutual Authentication and Key Agreement

Users should be able to authenticate other users as well as the eNB, to withstand impersonation attack.

3.2.2 Data Confidentiality and Integrity

The confidentiality of the data shared between users and the integrity of the communication between the users and the eNB should be well protected and resist eavesdropping and fabrication.

3.2.3 Free-riding Resistance

No client user should be able to get their intended data freely from the proxy users.

3.2.4 Double-spending/redemption Resistance

No user should be able to generate a verifiable virtual check or get rewarded multiple times for one virtual check value.

3.2.5 Availability

The service always should be available for users and furthermore, users should not wait a long time to get the service.

The considered security assumptions are as follows.

Attacker Model: Attacker(s) could be either internal or external adversary(s) who participate in any malformed behaviors such as fabricating messages, trying to repudiate their malicious behavior, preventing data sharing with others (free riding), denying service to other users or network element entities, either individually or by colluding with other entities.
Trust Model: The backbone entities of the network like the eNB, MME, and HSS are assumed to be honest enough to follow the protocol and not to be compromised by attackers. No trust relationship is assumed among users.

3.3 Design Goals

To establish secure data sharing communication between users in D2D communication, we propose an incentive-aware lightweight secure data sharing protocol which connects adjacent users to each other in order to offload network-side traffic and also enhance the QoS. The proposed scheme should achieve the following goals.

3.3.1 Security

Security is a major objective in the proposed scheme; without security, the incentive mechanism could be abused by adversaries leading to economic losses or temporarily unavailable system. Therefore, the proposed scheme should provide the aforementioned security requirements and resist MitM, Replay, DoS, Impersonation, free riding and double spend-

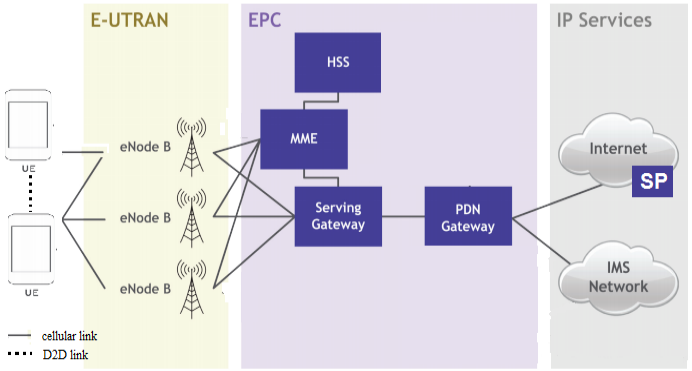

Figure 1. The Architecture of LTE-A networks

ing/redemption attacks.

3.3.2 Efficiency

The computation and communication overhead of the proposed scheme need to be minimized in terms of delay, CPU usage, and storage space. Additionally, concerning user mobility, the data transmission should be finished before users leave their home networks.

3.3.3 Fairness

The client will obtain the desired data with the minimum cost and the minimum waiting time whereas proxy will get enough credit every time they cooperate in data sharing scheme.

3.3.4 Mobility

As the proposed protocol should support user mobility, it should not depend on any historical data of the users. In such a stateless system, users can start using the service at anytime and from anywhere. Moreover, inter-operator and roaming scenarios based on [25] classification should be considered as well.

3.4 Cryptography Preliminaries

3.4.1 Authentication and Key Agreement (AKA) in LTE-A

The authentication procedure, EPS-AKA, is of two phases: (1) authentication data distribution and (2) user AKA. The first step enables the serving network (SV) which the user is visiting, to get access to the user's authentication data from its home network; and the second step establishes new session keys between the user and the SV. To authenticate users, a universal circuit card (generally known as SIM card), runs the universal subscriber identity module (USIM) that has access to the user's permanent key (K), where K is only known by USIM and AuC in the user's HSS. Therefore, HSS can generate the user's AV, through the EPS-AKA algorithm [11] for each received authentication request. Generally, the EPS-AKA algorithm takes the user's permanent key (K), a random number $RAND$, a sequence number SQN and the user's serving network identity $SNID$ as input, then outputs the user's authentication vector containing $AUTN$, RES and K_{asme}. Both the user and HSS are able to use the EPS-AKA algorithm. K_{asme}, an important parameter of AV, which is used to generate the user's integrity and confidentiality keys via a Key Derivation Function (KDF) [12] during future steps. For more detail, we refer the interested readers to [11].

3.4.2 Bilinear pairing

Let G_1 and G_2 denote two multiplicative cyclic groups of prime order q. Let g_1 and g_2 be two generators of G_1 and G_2, and let $e : G_1 \times G_1 \rightarrow G2$ be a bilinear mapping with the following properties.

- Bilinearity. For all $P, Q \in G_1$ and $a, b \in Z_q^*$, $e(P^a, Q^b) = e(P, Q)^{ab}$.
- Non-degeneracy . $e(P, Q) \neq 1_{G_2}$
- Symmetric. $e(P, Q) = e(Q, P)$ for all $P, Q \in G_1$
- Computability. There is an efficient algorithm to compute $e(P, Q)$. To implement a bilinear map e we can use the Weil [33] or Tate [34] pairings on elliptic curves.

4 The Proposed approach

In this section, we describe the details of the proposed protocol. The notations used in this paper are listed in Table 1.

4.1 Overview

A client user equipped with a device is willing to download a file from a device in its vicinity with the help of the operator. Therefore, the client user loads a virtual check and sends a download request to the eNB. The eNB gets the list of users within the client

user's proximity from the GW and performs a choose-candidate function to select the best pair for the client based on their location, mobility features and the cost of data transmission. Then, the eNB informs the chosen candidate (a proxy user) to transmit the data to the client user. Finally, if the originality of the received data is verified and confirmed by the client user, the proxy user is rewarded on his billing payments.

4.2 Fairness Model

To motivate users to use our service either as a client user or as a proxy, the following hybrid incentive mechanisms are adopted.

4.2.1 Payment Strategy

To motivate proxy users to share their data with the clients, we utilize "virtual check" which prevents the client from unbilling the âĂIJcheckâĂİ and knowing the exact amount of the check (the transmission cost) that should be paid to the proxy user. Moreover, to reduce the risk of payment, in case of malicious proxy, the proxy user will be able to deposit the âĂIJcheckâĂİ only if it honestly shared its data with the client user.

4.2.2 Best Candidate Selection

To motivate client users to get their data through D2D communication, rather than direct downloading from the internet, operators should consider some discounting mechanisms [16]. To further stimulate, in our service, eNB chooses the proxy user concerning the minimum cost of data transmission which could be paid by the client user. Therefore, it reduces the cost of using our service for the clients.

4.3 Proposed Protocol

In this section we describe the details of the system initialization and data sharing protocol.

4.3.1 System Setup

The trust authority chooses a symmetric encryption algorithm $Enc(*,k)$, an HMAC function $h(*,k)$ and two hash functions of $H_1 : \{0,1\}^* \rightarrow G$ and a simple one-way hash function $h(.)$; it then publishes the system parameters(Enc, h, H_1, g, G, q) where g is a generator of G (a multiplicative cyclic group of prime order q). The data packets are indexed by their frame numbers (especially for large video files) denoted by P_i. To guarantee data originality, SP computes a signature σ_{sp} over the data frames through $\sigma_{sp} = H_1(P_i \parallel M)^{x_0}$.

Table 1. The Notations used in the proposed protocol

Notation	Description
PID_i	Peer identity of user i
RID_i	Real identity of user i
$h(*,k)$	A secure HMAC function with the key k
$k_{upi,i}$	UE_i's integrity key for user plane connections
$k_{upc,i}$	UE_i's confidentiality key for user plane connections
$k_{cpi,i}$	UE_i's integrity key for control plane connections
$k_{cpc,i}$	UE_i's confidentiality key for control plane connections
P_i	The index of data
σ_{sp}	The service provider signature over an original message M
$Enc(*,k)$	A symmetric encryption algorithm with key k
T_s	Time-stamp
X_0, x_0	SP's public and private keys
X_1, x_1	eNB's public and private keys
$h(\cdot)$	a One-way hash function
VC	A virtual check value
$price_j$	UE_j's bid value to accept a sharing request

4.3.2 Secure Data Sharing

Users are assumed to be authenticated through an EPS-AKA before they start using our service; therefore, a secret session key $K_{asme,i}$ is shared between user UE_i and eNB. Furthermore, for those users who are subscribed to a different operator or roaming to a remote region, we utilize the secure UAKA protocol [25]. Our secure data sharing protocol for D2D communication, shown in Figure 2, consists of the following steps.

Step (1) *Service request.* To get the intended data with the portion index P_i, UE_i chooses a random integer $rand_i$ and generates a virtual check VC. Then, it sends the service request as $(PID_i, rand_i, P_i, Tsr, VC, h(*, K_{cpi,i}))$, where $K_{cpi,i}$ is UE_i's integrity key used at control plane side and is derived through the KDF. In particular, the KDF outputs two key pairs $(K_{cpi,i}, K_{cpc,i})$ and $(K_{upi,i}, K_{upc,i})$ from the generated secret key $K_{asme,i}$ and $rand_i$. The first key pair will be used to preserve data integrity and confidentiality in the control plane communication, while the second pair is used for integrity and confidentiality of the user plane communication (between UE_i and eNB).

Step (2) *Authentication and pair detection* . The eNB runs a KDF using $rand_i$ and shared key $K_{asme,i}$ to get the keys in order to check the integrity of the received message from UE_i. If the integrity check is passed, eNB sends the user's ID to the GW to get a list of users that are close to

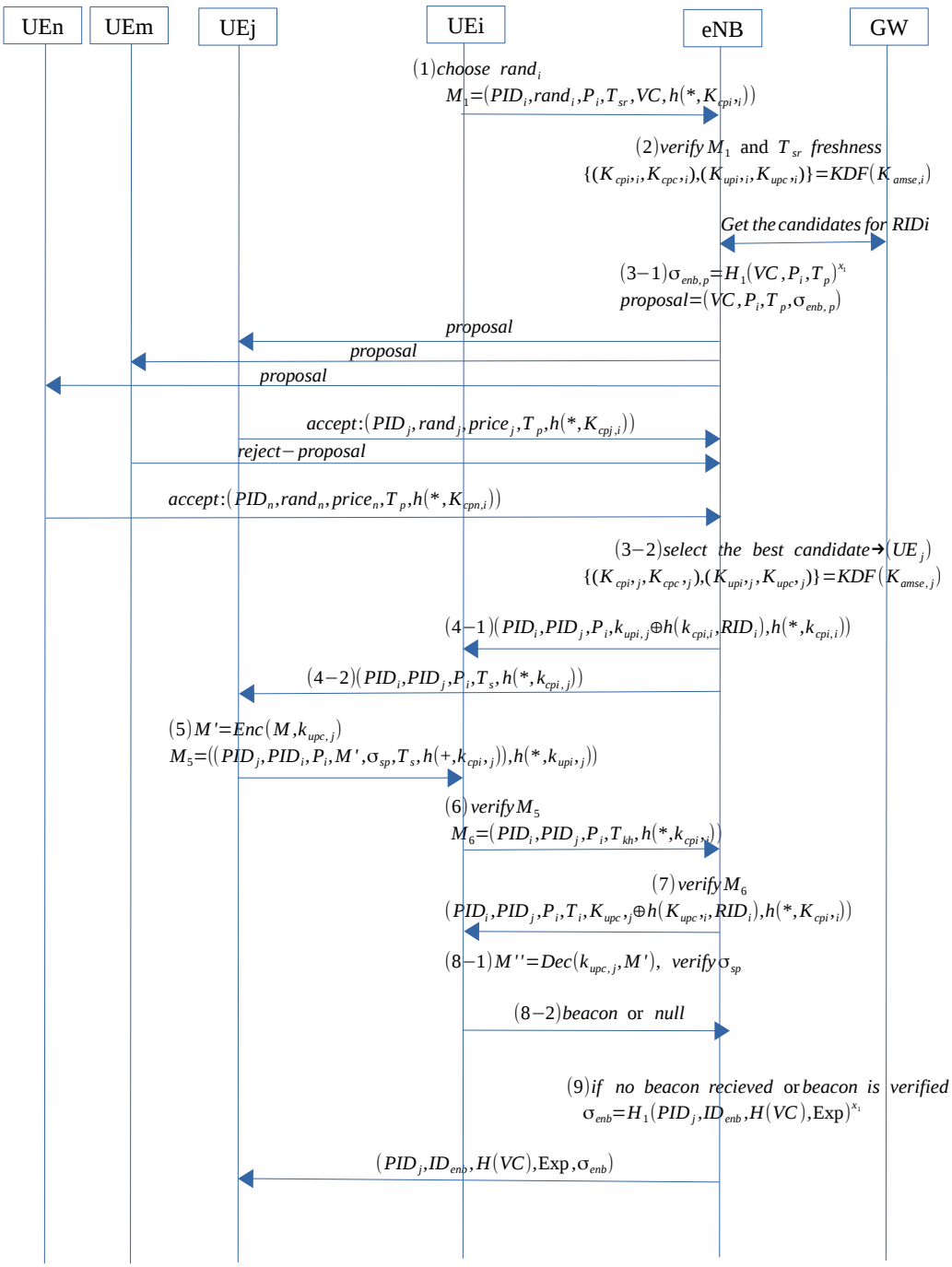

Figure 2. proposed protocol

UE_i. Otherwise, the request is ignored. Peer discovery by the GW is performed via PSCF according to [27].

Step (3) *Pair selection.* From the received list, eNB first filters those users who are holding a secure session key with the eNB. Then, eNB sends the proposal request containing $(VC, P_i, T_p, \sigma_{eNB,p})$ to them. jth candidate user, UE_j, can either accept or reject the received proposal. If UE_j has P_i and is eager to accept the proposal, it sends an accept request containing $(PID_j, rand_j, price_j, T_p, H(*, k_{cpj,i}))$; where $price_j$ is the intended benefit for UE_j to share its data with UE_i. eNB selects the best candidate from the users who accept the proposal using :

$$Min(price_k - face\_value)\ \forall\ k \in candidate\ list \quad (1)$$

$$where$$

$$\frac{Length_{P_i}}{Rate_{UE_k}} \leq \frac{eNB\_coverage}{Speed_{UE_k}}$$

eNB chooses the proper candidate (UE_j), which has the lowest bid, as a proxy user for UE_i; and UE_j is able to transmit the data before leaving the corresponding eNB. For example if UE_j's communication rate ($Rate_{UE_j}$) reaches 100 Mbps [28], to share 1G of data ($Length_{P_i}$), 10 seconds are needed. So, if the eNB covers an area of 500m * 500m (where $eNB\_coverage$ is 500m), and the speed of UE_j ($Speed_{UE_j}$) is about 50 Km/h, UE_j will leave the eNB in 36 seconds. Therefore, it could be a proper candidate for UE_i.

Step (4) *Device pairing.* eNB makes the response $(PID_i, PID_j, P_i, (k_{upi,j} \oplus h(k_{cpi,i}, RID_i)), h(*, k_{cpi,i}))$ for UE_i where the HMAC value $h(*, k_{cpi,i})$ ensures message integrity; $(k_{upi,j})$ is the UE_j's integrity key and makes it possible for UE_i to verify UE_j's message integrity in step 6. This key is XOR coded with UE_i's real ID and its integrity key($k_{cpi,i}$) through $k_{upi,j} \oplus h(k_{cpi,i}, RID_i)$.
eNB will also send a message containing $(PID_j, PID_i, P_i, h(*, k_{cpi,j}))$ to UE_j to notify it about UE_i's request. eNB should run a KDF using $rand_j$ and the shared key $K_{asme,j}$ to get UE_j's integrity and confidentiality keys such as $k_{cpi,j}$.

Step (5) *Data sharing.* By obtaining a data sharing request from eNB, UE_j first checks the integrity of the message. Then, UE_j encrypts the data M (related to the index P_i) through $M' = Enc(M, k_{upc,j})$, and sends the message $((PID_j, PID_i, P_i, M', \sigma_{sp}, T_s, h((PID_j, PID_i, P_i, M', \sigma_{sp}, T_s), k_{cpi,j})), h(*, k_{upi,j}))$ to UE_i. The outer HMAC value, $h(*, k_{upi,j})$, can be verified by UE_i and the inner one $(h((PID_j, PID_i, P_i, M', \sigma_{sp}, T_s), k_{cpi,j}))$ is generated to be verified by the eNB in case of any doubt (i.e., a message modification reported by UE_i to the eNB in step 8).

Step (6) *Entity Verification.* While receiving UE_j's message, UE_i first verifies message integrity by using UE_j's integrity key $k_{upi,j}$ received from the eNB in step 4. After that, UE_i sends a key hint request to the eNB to get the data encryption key through $((PID_i, PID_j, P_i, T_{kh}), h(*, k_{cpi,i}))$

Step (7) *Data verification.* When a key hint request is received by the eNB, it first checks the freshness of the attached time stamp and then the integrity of the message through $h(*, k_{cpi,i})$. If it is verified, then eNB makes a response to send the data encryption key to UE_i. The format of the response message is $(PID_i, PID_j, P_i, T_i, (k_{upc,j} \oplus h(k_{upc,i}, RID_i)), h(*, k_{cpi,i}))$. T_i is the time stamp that informs eNB about the time when the intended data was sent to UE_i (checked in step 9).

Step (8) *Receive confirmation.* UE_i can access the encryption key $k_{upc,j}$ by computing $h(k_{upc,i}, RID_i)$ using its confidentiality key XORing it with $(k_{upc,j} \oplus h(k_{upc,i}, RID_i))$, then it decrypts M'. Following this, it checks the validity of σ_{sp} through $\hat{e}(X_0, H_1(P_i \parallel M'')) \stackrel{?}{=} \hat{e}(\sigma_{sp}, g)$. If it is verified, it sends no feedback to eNB; otherwise it sends a beacon message by forwarding the received message in step 5 attached to an HMAC value with the key $k_{cpi,i}$, in an allowable window time to the eNB.

Step (9) *Billing Payment.* During the waiting time $(T_s + \Delta T)$ [20], if a beacon message is received, then eNB decrypts the message M' and verifies SP's signature (σ_{sp}). If the signature is verified, eNB confirms $UE_j's$ VC and delivers the message $(PID_j, ID_{enb}, H(VC), diff, Exp, \sigma_{enb})$ to UE_j, where $diff$ shows the difference between $price_j$ and the *face value* of VC. Otherwise, eNB refuses to bill the VC for UE_j.[3] It should be noted that, proxy users will obtain their credit only if the value of VCs would be successfully verified.

5 Evaluation and Results

In this section, we show that our proposed protocol outperforms previous studies in terms of security and efficiency.

5.1 Security Analysis

To investigate the security of the proposed protocol, we will assess how our protocol meets the security requirements related to our research context and its resistance to attacks.

5.1.1 Authentication and Key Agreement

We utilize an instance of the EPS-AKA algorithm to authenticate users in our protocol; thus, given the secrecy and uniqueness of the user's permanent key (K), which is only known by the user and its subscriber, there is no way to generate a verifiable version of AV without information about the user's private key (K). Therefore, only the user and its subscriber can get access to the authentication vector to derive the integrity and confidentiality keys during the data sharing protocol.

[3] If the eNB receives no feedback as a response from UE_i during the waiting time, it is assumed that the data is correctly delivered to UE_i

5.1.2 Confidentiality and Integrity

Confidentiality must be guaranteed for the user's data both in the key agreement and data sharing phases. Based on the EPS-AKA algorithm, the confidentiality of the cipher key is guaranteed and by encrypting the data through $Enc(M, k_{upc,j})$ in step 5, the confidentiality of the data is ensured as well. In addition, the key hint response in step 7, is sent over as $(k_{upc,j} \oplus h(k_{upc,i}, RID_i)$, which not only gives no information about the data sharing key $k_{upc,j}$ but also, due to the collision resistance of the one-way property of $h(.)$, it is a computationally infeasible problem for the adversary to derive the data encryption key $k_{upc,j}$.

To satisfy integrity service, all transmitted messages of the proposed protocol, are attached with a verifiable HMAC value by using the user's integrity keys both on control and data signaling. However, UE_j's integrity key for the user plane ($k_{upi,j}$) is shared with UE_i, in the proposed protocol, as a result of using the integrity key $k_{cpi,j}$ over the message transmitted in step 5 (which is only known by UE_j and eNB), any modification on the data by either adversaries or UE_i is detectable. Furthermore, according to the payment clearance process in which the integrity and authenticity of the virtual check VC are verified (by checking the eNB's signature), any modification could be detected. It should be noted that, we only consider the integrity of the price values and ignore the confidentiality to motivate other users to accept the proposal with a lower price than others in order to raise their chances in pair selection process.

5.1.3 Attack Resistance

The attack resistance of the proposed protocol is described below:

- **Man-in-The-Middle Attack**. If an adversary wants to get its intended data using a client user's virtual check; it should alter the communication between the victim client and the eNB by replacing its intended data e.g P_a with P_i in step 1. However, doing so results in invalidating the HMAC string of the message; also, the adversary cannot generate a correct message authentication code by himself because he has no clue about the secret integrity key of the client. Moreover, an adversary cannot intervene in the direct communication between users in step 5, as a MitM, because he should generate a verifiable value of $h(k_{cpi,i}, RID_i)$ and since he does not have access to the secret UE_j's integrity key, he should be able to compute a preimage of the $k_{upi,j} \oplus h(k_{cpi,i}, RID_i)$ which is captured during step 4; meanwhile, this is computationally infeasible.
- **Replay Attack**. In the proposed protocol, most of the messages are attached with a time stamp value. Therefore, any replay attempts from an attacker would be easily detected by checking the freshness of the time-stamp. In addition, the expiration time Exp and the unique identity of the used virtual check according to [10] prevents an attacker from resending an eavesdropped message.
- **DoS Attack**. Although HSS could be a bottleneck of the EPS-AKA protocol, we have improved our previous work [21] and removed running the EPS-AKA per data sharing session. In particular, we assume that users are being authenticated before starting to use the service; so, users just need to perform EPS-AKA per location-update which is less frequent. Besides, during the pair selection procedure, eNB becomes more involved than the other steps, which may lead a number of attackers to send many valid service requests to the eNB concurrently. Therefore, eNB should generate a proposal per request and send it to a group of chosen users as candidates. However, the proposal message is pretty short and only needs a valid signature of the eNB; so, it does not take very long to compute. Thus, even if there were many candidates who wish to accept the proposal, the computation overhead of choosing the best candidate through Equation (1) is pretty lightweight. Therefore, given the computation power of the eNB, even a group of legal users who simultaneously generate valid requests to the eNB may not cause interruptions or service unavailability.
- **Impersonation Attack**. An adversary will not be authenticated by the eNB, unless it is able to get access to the users secret shared session key K_{asme} and derive related keys as a legal user can. With respect to the security of EPS-AKA, attacker(s) cannot carry out an impersonation attack. Additionally, sniffed packets that are retransmitted will be dropped by eNB given the presence of a time-stamp and a random number.
- **Free-riding Attack**. A client user cannot obtain the desired data without paying for it. Specifically, the client should load a valid virtual check VC together with his service request in step 1. He cannot access the decrypted data in step 5 until a key hint request is sent to the eNB (in step 6). Therefore, he cannot refuse to bill the proxy user if the originality of the received data is verified.
- **Double spending/redemption attack**. When a proxy user shares its data correctly with

the client user, it can get the eNB's signature over the message $(PID_j, H(VC), diff, Exp)$. Based on the digital signatures, it holds non-repudiation for billing. Given the uniqueness of the VC's identity, no VC could be paid more than once and regarding the existence of PID_j, even eavesdropped messages cannot result in charging any other user except UE_j.

5.2 Performance Evaluation

We evaluate the computation and communication overhead used to provide security protection in the proposed data sharing protocol.

5.2.1 Computation Cost

As mobile devices are resource-constrained, we adopt a symmetric cryptosystem rather than using public key cryptosystem, because it is much faster than public key cryptosystem and also requires a smaller secret key length with the same level of security. Accordingly, we strive to minimize computation costs in order to achieve better efficiency.

The dominant computation costs of the proposed protocol are pairing execution for SP and eNB's signatures verification; while the other computation overhead is purely symmetric. To protect the integrity of the message, a message authentication code is generated in steps 1,3,4,5,6,7, and 8. To protect file confidentiality, a symmetric encryption algorithm used in step 5. All MAC computations as well as symmetric-key encryption and decryption, are negligible compared to the pairing operation.

A secure data sharing protocol proposed by Zhang et al. known as SeDS[20] and the recent study of [21] are quite similar to the present study. SeDS uses a public key-based digital signature for user authentication and a symmetric encryption algorithm for data confidentiality. On the other hand, in [21], users are authenticated through an EPS-AKA which is more lightweight than public key cryptosystem.

Table 2 compares the overall computation costs among the proposed protocol, SeDS and the protocol in [21].

Let T_{mul} stand for the time of one multiplication execution in G. Therefore, according to [35], the computation cost of $T_{KDF} \approx T_{MAC} \approx 1.5T_{mul}$. The expensive computational costs are $T_{pair} \approx 15T_{mul}$ and $T_{exp} \approx 92.5T_{mul}$[36]. So as listed in Table 2, the overall computation cost of HSS and eNB in [21] are about $22.5T_{mul}$; the computation cost of the eNB in SeDS is about $194T_{mul}$. [4] ; and the computation cost of the eNB in our scheme is $45T_{mul}$. The computation cost of UE_i in [21] is about $43.5T_{mul} + T_{Dec}$ whereas it is about $160T_{mul} + T_{Dec}$ in the SeDS and $42 + T_{Dec}$ in the proposed scheme.

Finally, UE_j spends $19.5T_{mul} + T_{Enc}$ for computation cost while in the SeDS, it is about $203T_{mul} + 2T_{Enc}$ and about $9T_{mul} + T_{Enc}$ in [21]. The comparison of computation cost of our scheme and [20] and [21] are tabulated in Table 3. So, the proposed protocol and [21] are much suited for mobile devices than SeDS due to lower computational cost. Given the high computational capacity of the eNB, it's higher computation cost in our scheme compared to SeDS and [21] could be ignored. Note that, in the proposed protocol, to support user mobility we remove the need for keeping historical user data which is done by the eNB in SeDS and [21].

5.2.2 Communication Cost

In Table 4, the communication overhead of the proposed scheme is compared with that of SeDS[20] and [21]. The communication required for getting service by UE_i is 42+32 bytes, where the numbers show the number of bytes for the service request and the number of bytes sent to get the key hint from the eNB, respectively. The proxy user UE_j, sends 48 bytes for proposal acceptance and 70+L bytes for data transmission to UE_i for L bytes of data. The communication overhead of the eNB consists of $2 + 32n_c$ for getting the list of the candidates from GW (where n_c represents the number of candidates) and sending the proposal to them; 46 bytes to respond to UE_i service request and 32bytes to inform the proxy user UE_j to share the data; finally, eNB is supposed to send a message containing the data encryption key to UE_i, causing 48 bytes overhead and should send the reward message to UE_j which causes 48 bytes overhead.

As shown in Table 3 and 4, the computation cost of the proposed protocol is a bit more than the protocol in [21], but our protocol communication cost is less than [21]. With respect to importance of the communication cost in comparison to computation cost in wireless networks [38], the proposed protocol outperforms SeDS protocol [20] in both communication and computation costs. So, our scheme is much suited for the resource-constrained mobile devices due to its low communication and computational cost among others.

5.3 Analysis of Incentive Mechanism

According to Equation (1), eNB selects the best candidate in terms of sharing price and mobility features.

[4] we ignore the T_{DEC} of the eNB in the SeDS because it is pretty lightweight (about $0.09T_{mul}$)

Table 2. The computational overhead comparison

entity	SeDS	Mohseni et al.[21]	Proposed Protocol
HSS	0	$4MAC + 4KDF$	0
eNB	$6MAC + 2EXP + 1DEC$	$5MAC + 2KDF + 1XOR$	$5MAC + 2PAIR + 3HASH + 2KDF + 2XOR$
UE_i	$5MAC + 4PAIR + 1EXP + 1DEC$	$7MAC + 2KDF + 2PAIR + 1DEC + 1XOR$	$5MAC + 2PAIR + 2HASH + 1DEC + 1KDF + 2XOR$
UE_j	$2MAC + 2ENC + 2EXP + 1PAIR$	$5MAC + 2KDF + 1ENC$	$2MAC + 1PAIR + 1ENC + 1KDF$

EXP: exponential computation ,PAIR: one pairing execution

Table 3. The comparison of overall computation time of users

scheme	overall computation time of users(ms)
SeDS [20]	$557T_{mul}$+3*T_{Enc}
[21]	$75T_{mul}$+2*T_{Enc}
our scheme	$106T_{mul}$+2*T_{Enc}

$T_{Enc} \approx T_{Des} \approx 2.8L * 10^{-5}$ms, for L bytes of data [37]

Table 4. The communication overhead comparison

entity	SeDS	Mohseni et al.[21]	Proposed Protocol
eNB	162+$2n_c$ Bytes	350+$2n_c$ Bytes	176+$32n_c$ Bytes
UE_i	74 Bytes	98 Bytes	74 Bytes
UE_j	116+L Bytes	74+L Bytes	118+L Bytes

The virtual check value VC consists of a unique identity and a face value chosen by the client user[10]. Using VC eliminates the demands of accurate knowledge of the exact amount of the check. Moreover, to motivate proxy users to help the client user, they also bid their desired prices $price_j$ according to the face value of VC. Regarding the pair selection mechanism in the eNB, the candidate pair with the minimum value of $(price_j - face\_value)$ is chosen. The chosen value of each candidate user $price_j$ is sent without encryption protection [5] , so it can motivate the users to bid lower than $price_j$ in order to increase their chance of being chosen.

As investigated in [39], mobility can affect energy and bandwidth efficiency in D2D communication. Furthermore, delay-tolerant applications like file sharing, are sensitive to the type of user mobility[40]. Therefore, we also consider the mobility features of the proxy user like $RATE_{UE_j}$, to ensure that both the client and the proxy users will stay in the eNB coverage until the data sharing procedure is finished. To extend accuracy, we can adopt the mobility model presented in [41]. Accordingly, our proposed incentive mechanism is effective.

[5] however, the integrity of the message is guaranteed using MAC

6 Conclusion

In this paper, an incentive-aware lightweight secure scheme was proposed to achieve secure, fair, and reliable data sharing in D2D communication. By adopting a payment strategy using "virtual check", the proposed scheme can achieve fairness among the users. Users should be authenticated through an instance of EPS-AKA named UAKA [25] which supports roaming and inter-operator modes. Based on the secret shared key between each user and the eNB, two pairs of keys would be derived; these key pairs preserve data integrity and confidentiality of the messages of the control and data planes. A symmetric encryption algorithm guarantees data confidentiality while a MAC function ensures that message integrity and data origin authentication. To motivate users to share their data with the client user, a payment mechanism is considered in which only those users who get involved in a successful data sharing scheme can obtain their credits. Moreover, the trust authority chooses the best candidate to share the data with the client user in a fair manner by considering a balance between the price that a client user wishes to pay and the price that a proxy user wants to receive. Finally, the proposed scheme is compatible with user mobility; thus, our protocol is more reliable and practical than previous works. The evaluation results prove the security and the efficiency of the proposed protocol. In a nutshell, the proposed protocol guarantees data confidentiality and integrity and resist message fabrication, man-in-the-middle, replay, free-riding, and DoS attacks with an acceptable performance by decreasing the computation cost of users compared with previous works.

For the future works, we will consider a reputation scheme to get more reliable service by revoking malicious users. Moreover, we will try to propose a scheme which does not rely on time-synchronized entities.

References

[1] Cisco,*Cisco Visual Networking Index: Global Mobile Data Traffic Forecast Update* , 2015-2016,âĂİ Cisco, USA, Feb 2016.

[2] Andrews et al., "What will 5G be?." IEEE Journal on selected areas in communications 32.6 (2014): 1065-1082.

[3] Mohseni-Ejiyeh, Atefeh, and Maedeh Ashouri-Talouki. "SeVR+: Secure and privacy-aware cloud-assisted video reporting service for 5G vehicular networks." Electrical Engineering (ICEE), 2017 Iranian Conference on. IEEE, 2017.

[4] Aijaz, Adnan et al., *A survey on mobile data offloading: technical and business perspectives*,IEEE Wireless Communications, Vol 20, pp 104-112,2013.

[5] Andreev, Sergey, et al., *Cellular traffic offloading onto network-assisted Device-to-Device connections*, IEEE Communications Magazine,Vol 52, pp 20-31,2014.

[6] Asadi, Arash, et al., *A survey on Device-to-Device communication in cellular networks*, IEEE Communications Surveys and Tutorials, Vol 16, pp 1801-1819,2014.

[7] Wang, Mingjun, and Zheng Yan, *A survey on security in D2D communications*, Mobile Networks and Applications,1-14,2016.

[8] Naslcheraghi, Mansour, et al., *FD Device-to-Device communication for wireless video distribution*, IET Communications, Vol 11, pp 1074-1081, 2017.

[9] Golrezaei, Negin, et al. "Femtocaching and Device-to-Device collaboration: A new architecture for wireless video distribution." IEEE Communications Magazine, Vol 51, pp 142-149, 2013.

[10] Ning, Ting, et al. "Self-interest-driven incentives for ad dissemination in autonomous mobile social networks." INFOCOM, 2013 Proceedings IEEE. IEEE, 2013.

[11] 3GPP, TR 33.401, v.14.2.0, *Security Architecture*, Release 14, 2017

[12] 3GPP, TS 33.105 version 14.0.0, *Cryptographic Algorithm Requirements*, Release 14, 2017

[13] Hossain, Ekram, et al., *Evolution toward 5G multi-tier cellular wireless networks: An interference management perspective*, IEEE Wireless Communications, Vol 21, pp 118-127,2014.

[14] Choi, Kae Won, and Zhu Han, *Device-to-Device discovery for proximity-based service in LTE-advanced system*, IEEE Journal on Selected Areas in Communications, Vol 33, pp 55-66, 2015

[15] Wang, Mingjun, and Zheng Yan. *A survey on security in D2D communications*, Mobile Networks and Applications,Vol 22, pp 195-208, 2017.

[16] Tehrani, Mohsen Nader, et al., *Device-to-Device communication in 5G cellular networks: challenges, solutions, and future directions*, IEEE Communications Magazine, Vol 52, pp 86-92, 2014.

[17] Zhang, Aiqing, et al., *Light-weight and robust security-aware d2d-assist data transmission protocol for mobile-health systems*, IEEE Transactions on Information Forensics and Security, Vol 12, pp 662-675, 2017.

[18] Li, Feng, Jie Wu, and Anand Srinivasan. *Thwarting blackhole attacks in disruption-tolerant networks using encounter tickets*, INFOCOM 2009, IEEE. IEEE, 2009.

[19] Schmittner, Milan, et al., *SEMUD: Secure Multihop Device-to-Device Communication for 5G Public Safety Networks*, IFIP, 2017.

[20] Zhang, Aiqing, et al., *SeDS: Secure data sharing strategy for D2D communication in LTE-Advanced networks*, IEEE Transactions on Vehicular Technology,Vol 65, pp 2659-2672, 2016.

[21] Mohseni-Ejiyeh, Atefeh, Maedeh Ashouri-Talouki, and Mojtaba Mahdavi. "A Lightweight and Secure Data Sharing Protocol for D2D Communication." Information Security and Cryptology (ISCISC), 14th International Iranian Society of Cryptology Conference on. IEEE, 2017.

[22] Zhang, Yanru, et al. "Contract-based incentive mechanisms for Device-to-Device communications in cellular networks." IEEE Journal on Selected Areas in Communications, Vol 33, pp 2144-2155, 2015.

[23] Wang, Yan, Mooi-Choo Chuah, and Yingying Chen. "Incentive based data sharing in delay tolerant mobile networks." IEEE Transactions on wireless communications, Vol 13, pp 370-381, 2014.

[24] Zhao, Yiming, Wei Song, and Zhu Han. "Social-aware data dissemination via Device-to-Device communications: Fusing social and mobile networks with incentive constraints." IEEE Transactions on Services Computing (2016).

[25] Wang, Mingjun,et al., *UAKA-D2D: Universal Authentication and Key Agreement Protocol in D2D Communications*, Mobile Networks and Applications, pp 1-16, 2017

[26] Alam, Muhammad, et al. *Secure Device-to-Device communication in LTE-A*, IEEE Communications Magazine, Vol 52, pp 66-73, 2014.

[27] Yang, Mi Jeong, et al., *Solving the data overload: Device-to-Device bearer control architecture for cellular data offloading*, IEEE Vehicular Technology Magazine, Vol 8, pp 31-39, 2013.

[28] Ghosh, Amitava, et al. "LTE-advanced: next-generation wireless broadband technology." IEEE wireless communications, Vol 17, 2010.

[29] Han, Chan-Kyu, and Hyoung-Kee Choi., *Security analysis of handover key management in 4G LTE/SAE networks*, IEEE Transactions on Mobile Computing, Vol 13,2014

[30] Lai, Chengzhe, et al. "SE-AKA: A secure and efficient group authentication and key agreement protocol for LTE networks." Computer Networks, Vol 57, pp 3492-3510, 2013.

[31] Alezabi, Kamal Ali, et al. "An efficient authentication and key agreement protocol for 4G (LTE)

networks." Region 10 Symposium, 2014 IEEE. IEEE, 2014.
[32] Soran Sabah Hussein; Lightweight Security Solutions for LTE/LTE-A Networks; PHD thesis, Paris-SUD University, 2014
[33] Boneh, Dan, Ben Lynn, and Hovav Shacham. "Short signatures from the Weil pairing." Advances in CryptologyâĂŤASIACRYPT 2001 (2001): 514-532.
[34] Scott, Michael. "Computing the Tate pairing." Topics in CryptologyâĂŞCT-RSA 2005 (2005): 293-304.
[35] Chatterjee et al., *An Enhanced Access Control Scheme in Wireless Sensor Networks*, Adhoc and Sensor Wireless Networks, Vol 21, 2014.
[36] Hsu, Ruei-Hau, et al. *GRAAD: Group Anonymous and Accountable D2D Communication in Mobile Networks*, arXiv preprint arXiv:1703.04262, 2017.
[37] Scott, Mike. *Efficient implementation of cryptographic pairings*, Online]. http://www. pairing-conference. org/2007/invited/Scott slide. pdf. 2007.
[38] De Meulenaer, Giacomo, et al. "On the energy cost of communication and cryptography in wireless sensor networks." Networking and Communications, 2008. WIMOB'08. IEEE International Conference on Wireless and Mobile Computing, IEEE, 2008.
[39] Wu, Dan, et al. *The role of mobility for D2D communications in LTE-Advanced networks: energy vs. bandwidth efficiency*, IEEE Wireless Communications, Vol 21, (2014): 66-71.
[40] Orsino, Antonino, et al. "Direct Connection on the Move: Characterization of User Mobility in Cellular-Assisted D2D Systems." IEEE Vehicular Technology Magazine, Vol 11, pp 38-48, 2016.
[41] Wang, Rui, et al. "Mobility-aware caching in D2D networks." IEEE Transactions on Wireless Communications, Vol 16, pp 5001-5015 ,2017.

Atefeh Mohseni-Ejiyeh received her B.S. degree in information technology engineering from University of Isfahan, Isfahan, Iran in 2015. She is currently an M.S. student in information security in faculty of computer engineering at the University of Isfahan. Her research interests lie in the areas of mobile network security, security applications for D2D communication, lightweight cryptography and cryptanalysis.

Maede Ashouri-Talouki is an assistant professor of information technology engineering Department of University of Isfahan. She received her B.S., M.S., and Ph.D. degrees in computer engineering from University of Isfahan in 2004, 2007 and 2012, respectively. In 2013, she joined University of Isfahan. Her research interests include mobile networks security, user privacy and anonymity, cryptographic protocols and network security.

Mojtaba Mahdavi received the B.S., M.S. and Ph.D. degree in computer engineering from Isfahan University of Technology, Isfahan, Iran, respectively, in 1999, 2002 and 2011. His research interests are in the area of network security, data hiding (steganography and watermarking) and wireless networks. He is currently with the department of information technology engineering at University Isfahan, Isfahan, Iran.