Abstract—D2D is one of the fast developing methods of cellular communication. Experiments and development in this particular model will create a new standard of communication in this modern world. As the data theft is one of the major threat in case of any mode of communication. In this paper, we propose a secure data sharing protocol, it merges the advantages of public key cryptography and symmetric encryption, to achieve data security in D2D communication. Particularly, public key based digital signature combined with mutual authentication mechanism of cellular network promises the entity authentication, transmission non-repudiation, traceability, data authority as well as integrity. Data confidentiality is also ensured by employing the symmetric encryption method. A key feature of the protocol proposed is that it can detect free-riding attack by keeping a record of the current status for the user equipments (UEs) and realize reception non-repudiation by key hint transmission between the UE and evolved NodeB, thus improving the system availability.

Keywords—D2D communication, authentication, non-repudiation, digital signature

I. INTRODUCTION

The past few years have witnessed a drastic growth of mobile user population as well as multimedia services, which have resulted in a severe traffic overload problem in the traditional cellular network. Device-to-Device (D2D) communication is a technique that has been proposed to be a promising data offloading solution and spectrum efficiency enhancement method due to its inherent characteristics, like – improving the resource utilization, enhancing user’s throughput, extending battery lifetime, etc. Accordingly, it has also drawn considerable attention in research community in recent years. Besides the conventional cellular operation where user equipments (UEs) are served directly by the evolved NodeB (eNB), user equipments are also able to communicate directly with each other over the D2D link which is quite different from the traditional D2D communication techniques. D2D communication under-laying LTE-Advanced (LTE-A) networks actually works on a licensed band, which usually provides a planned deployment instead of an uncoordinated ones, resulting in a better user experience along with the guarantee of service. Therefore, it is necessary as well as important to develop new functions and applications with the assistance of cellular networks.

Despite of all the advantages, D2D communication still faces two substantial technical challenges when it is applied in large-scale, security and availability. As the connections happen directly between the proximity devices, D2D communication is subjected 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 leads to serious consequence as well as to deteriorated user experience. Intermittent connection and long waiting time for sharing the information are also to be taken care of in order to provide a better experience for the users. 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 above 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 communication.
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 non-repudiation as well as offering evidence for the data sharing event, which is employed to resist free-riding attack and improve system availability.

II. BACKGROUND

Long term evolution (LTE) technology brings cellular communications to the fourth generation (4G) era. This standard specification has been proposed by the third generation partnership projects (3GPP). The aim is to support reduced latency, high user data rate, improved system capacity and improved spectral efficiency. The current LTE system is studied and labeled as LTE-advanced (LTE-A) technology. This includes proximity services (Prose) which is the same concept of D2D communication. It is expected to be promising technology that serves future services or needs e.g., Public safety, social networking. Even though demand has increased energy consumption is a growing concern. A device has to support both cellular and D2D communication i.e. additional energy is required. The recent device supports multiple radio access technologies i.e. multiple modem, RF chain and antennas are implemented in one device. Further LTE A shows highest UE energy consumption compared with Wi-Fi or WCDMA.

D2D communication may be of three types
- Peer to peer communication: This is point to point communication and most studies on D2D communication consider this type of transmission.
- Cooperative communication: This uses mobiles as relays to extend coverage, and exploits cooperative diversity through multiple collaborative mobiles to obtain space diversity.
- Multiple-hop (multihop) communication: This is similar to mobile ad-hoc network and mesh network, which may include complex data super position, and data routing, e.g., wireless network coding.

A) Radio resource control (RRC)

The main function is to manage the connection between UE and network. The RRC states in LTE are simplified to two states RRC-idle and RRC-connected [1].
- RRC_IDLE – There is no connection between UE and evolved node B (eNB)
- RRC_CONNECTED – There is connection between UE and eNB.

B) Discontinuous reception (DRX)

In DRX mode, the UE powers down when there is no packet activity. In LTE-E and RRC connected state. When no data is sent or received during the connected UE performs DRX operation with short DRX cycle, where UE wakes up only periodically and sleeps for remaining time to save energy. If there is no DRX activity until the short DRX time expires the connected UE switches to long DRX mode which operates with a comparatively long cycle [1].

III. 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] while only very few efforts have been made on security issues [11]–[13]. Specifically, instead of interference mitigation and avoidance, the authors in [12] exploit interference against eavesdropping, which is an effective way to enhance information-theoretic secrecy capacity. This work is heuristic while it does not consider the security requirements of D2D pairs. [13] develops a coalitional game theoretic framework 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 work does not consider and analyze the
potential threats such as eavesdropping or fabricating.

IV. KEY TECHNOLOGIES FOR D2D COMMUNICATION

A) Configuration of D2D communications

D2D networks can be configured in the following three ways to allow or restrict their usage by certain users.

Network-Controlled D2D: In this scenario, the communication signaling setup and there after resource allocation for both cellular and D2D users are controlled by the base station (BS) and the core network. This centralized configuration benefits from efficient interference avoidance and resource management. However, when the number of D2D links becomes large this scheme incurs a large amount of control signaling, which can increase the overhead and reduce the spectrum efficiency. Therefore, this fully network controlled approach is particularly useful for scenarios with small numbers of D2D links.

Self-organized D2D: In this scenario, D2D users themselves realize the communication in a self-organizing way by finding the empty spectrum hole. This configuration is similar to cognitive radio, which allows D2D users to sense a surrounding environment, thereby obtaining CSI, interference, and cellular system information. This distributed method can effectively avoid the controlling signaling overhead, and the time delay, but the self-organized nature of this method cause communication chaos and instability due to lack of control by the operators in the licensed spectrum.

Network-assisted D2D: The D2D users operate in a self-organized way, and, for resource management, exchange with the cellular system a limited amount of controlling information. The cellular network can use the status of D2D communication for better control purposes. This approach has the merits of the first two approaches.

B) Device synchronization and discovery

For D2D communications, synchronization between cellular networks and D2D users and among D2D users will be necessary to minimize multiple access interference and for proper handoff. The approaches in IEEE 802.11 or in LTE can be adopted to enable the synchronization among mobiles. Typically, device synchronization and discovery are realized in a joint way. The fundamental problem of device discovery is that two devices have to meet in space, time, and frequency without any coordination. This can be made possible via some randomized procedure, and one of the peers assumes the responsibility of sending the beacon. For traditional peer discovery, both in the ad-hoc case and in the cellular case, the discovery is made possible by one party transmitting a known synchronization or reference signal sequence (the beacon). Depending on whether or not there are responses from the discovering UEs, the discovery approaches can be classified into two categories: beacon-based discovery and request-based discovery. According to whether there is network participation in the detection, the discovery procedure could be categorized into two types: network-assisted detection and non-network-assisted detection. In the case of network-assisted D2D, the network can mediate in the discovery process by recognizing D2D candidates, coordinating the time and frequency allocations for sending/scanning for beacons, and thereby making the pairing process more energy sufficient and less time consuming.

C) Mode selection: In a D2D underlay communications system, one of the most challenging problems is to decide whether communicating devices should use cellular or direct communication mode [8]. In the D2D mode, data is directly transmitted to the receiver while the cellular communication mode requires the source device to transmit to the eNB and then the destination device receives from the eNB on downlink (DL). Here, three different mode selection criteria are considered.

a. Cellular: All devices are in cellular mode.
b. Force D2D: D2D mode is always selected for all the communicating devices.
c. Path-loss D2D: D2D mode is selected if any of the path losses between a source device and its
serving eNB, or a destination device and its serving eNB, is greater than the path loss in the direct link between the source node and the destination node.

D) Spectrum sharing and resource management:
Spectrum sharing methods [8] for D2D communications can be categorized as follows.

**Overlay D2D communications:** The D2D users occupy the vacant cellular spectrum for communication. This approach can completely eliminate cross-tier interference by dividing the licensed spectrum into two parts (i.e., orthogonal channel assignment). That is, one fraction of sub channels will be used by the cellular users while another fraction would be used by the D2D networks. Although it is optimal from a cross-tier interference standpoint, this approach is inefficient in terms of spectrum reuse.

**Underlay D2D communications:** In the spectrum-sharing scheme, multiple D2D users are allowed to work as an underlay with cellular users, and thus improve the spectrum efficiency. Co-channel assignment of the cellular and D2D users will be more efficient for profitable for operators, although this is far more intricate than the overlay scheme from the technical point of view [8].

E) Power control: Power control is an important and effective way to coordinate the co-channel interference. Power control can be performed by two methods.

**Self-organized power control:** The D2D users make power changes in a self-organized way according to the predefined signal-to-interference-plus-noise ratio (SINR). Threshold in order to meet the QoS without affecting the cellular users.

**Network-managed power control:** Both cellular and D2D users adaptively adjust their transmit power according to the SINR report [1]. Typically, the D2D users can control the transmit power first, and then the cellular users make changes afterward. This iterative process terminates when all the users have satisfied their SINR requirements [8].

Obviously, the first method is not going to change the behavior of cellular users since the D2D users are treated invisibly. This method is simple, but less efficient than the second method, which allows all of the users to adjust their transmit powers. However, the network controlled approach requires some information exchange among cellular users, D2D users, and the eNB.

F) Device to device handoff: As in case of usual mobile handoff technique, in this process the device that is gaining signal from the virtual antenna will be handed over to any other adjacent UE by making it act as virtual antenna if the previous antenna receives a call [4]. For e.g., if there are three users in an area named UE1, UE2, and UE3. The UE1 wants to call any other user but does not have signal coverage, at this point of time it will transmit a beacon to the surrounding region requesting for signal. By then the BS will make a study over the nearby UEs and manages to find the nearby UE to which the UE1 can be connected and provided with the signal with. Let us consider that the UE2 is nearer than that of UE3, in this condition the UE1 will be instructed to connect with the UE2.

But when the UE2 receives a call an immediate handover to the next nearby device takes place, say UE3, without disconnecting the call of UE1. Hence handoff of the UEs is also designed using the beacon transmission itself.

V. ISSUES AND CHALLENGES IN D2D COMMUNICATIONS

For D2D direct, several key challenges are as follows [2].

- Scaling law and capacity analysis.
- Channel measurement and modeling, and interference analysis.
- Proximity-based applications, such as context-aware networks, and offload in concert and stadium networks.
- Mobility measurement, modeling, and management.
- Reduction of signaling overhead.
- Limited-backhaul issues for cross-cell D2D transmission.
One of the major difficulties hindering D2D communications is the need to develop efficient data spreading in the D2D networks without causing severe disturbance of the original cellular networks. Power control, cooperative transmission, and multiple-access methods need to be carefully researched. The use of wireless network coding has been recognized as an efficient way to improve the network performance in terms of spectrum efficiency, and thus the question of how to adopt this technique has to be studied carefully. For multihop D2D communications, which is particularly useful for coverage extension, it would be desirable to incentivize intermediate nodes to participate in a relaying process. In this case, a rewarding system regarding proper payment must be developed.

VI. CROSS-LAYER DESIGN FOR D2D COMMUNICATIONS

Traditional communication systems were built using a layered structure to provide well defined but limited interfaces among protocols in adjacent layers. The modular design of the layered structure, where the details of each protocol are hidden, promotes the interoperability of the communication protocols. Although the protocol details (e.g., states and internal functions) are encapsulated in each layer, this structure prevents the protocol sharing, accessing, and controlling the operations of other protocols, which might be required for efficient data transmission [3]. Therefore, the concept of cross-layer design has been introduced to allow tighter integration of different protocols. It is not necessary for these protocols to be in adjacent layers. The benefits of cross-layer design are that it allows one to improve both the flexibility of protocol implementation and network performance. The cross-layer design layer has been adopted for optimizing D2D communication [4]. One of the most commonly used cross layer design models, i.e., the coordination model, which incorporates different functionalities. These functionalities are security, QoS, mobility and wireless length adaptation.

VII. SYSTEM MODEL

A. Network Architecture:

To capture a general D2D communication scenario, similar to, 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 network. Thus the participators can download or share the data with their mobile phones using D2D communication.

Extensively, a D2D communication system includes four parts: GateWay (GW) and eNB of a cellular network, UEs of cellular users, and server of Service Provider (SP).

GW serves as the gate from the local subsystem to the core network. In addition to routing IP packets from/to the Internet, the gateway is able to detect the potential D2D traffic with Proximity Service Control Function (PSCF). The PSCF earmarks the traffic flows and look for pairs of D2D enabled devices.
The infrastructure connected to the mobile phone network and the GW, is a very important element in E-UTRA (Evolved Universal Terrestrial Radio Access) of LTE-A network. It is responsible for resource allocation of cellular network as well as 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 network. 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 and UEs2, are the peer entities of the D2D connections. The information available at the devices is shared among users by D2D communication 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 LTE-A network, UE is designed with the function

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

SP is proposed to provide authentic information at the beginning of the system establishment process. The informa-tion 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 to be completely trustable and can’t be comprised by the attackers. Moreover, SP is honest enough to provide correct source data while UEs may be comprised of or captured by some adversaries, the threats of which are analyzed in the next part.

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) attack. DoS attack in wireless communication networks has been extensively investigated during the past decades [24], [25]. Thus we will focus on the other security issues in D2D communication. Especially, 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 free-riding attack, which causes a serious threat and reduces the system availability of D2D communication.

VIII. SECURE DATA SHARING PROTOCOL

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

Step 1 Service request. A UE (called UEi), who intends to get the ith frame of the data, randomly selects $c \in \mathbb{Z}_q^*$ and computes the key hint $z = gc$ for generation of communication key $kc$, 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

$$HMAC_k(m) = h[(k+ \oplus opad) \| h[(k+ \oplus ipad) \| m]];$$

where $k+$ is the key padded out to size, and $opad = 01011110; 01011110; \ldots; 01011110,$ $ipad = 01011100; 01011100; \ldots; 01011100$ are specified

padding constants, $h(\cdot)$ is a cryptographic hash functions such as SHA-1.

Then UEi sends a service request message along with its PIDi, $z$ and the expected portion index Pi, namely (PIDi\| z\| Pi\| h[(k+ \oplus opad)\| h[(k+ \oplus pad)\| PIDi\| z\| Pi)], to the eNB.
(1) For the simplification of expression, \( h[(k+ \oplus \text{opad}) \parallel h[(k+ \oplus \text{ipad}) \parallel \text{PIDi} \parallel z \parallel \text{Pi}]] \) 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 UEi 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 firstly verifies its integrity and verification by computing hashed value of the message, and authenticates the requester in the normal cellular communication mode, obtaining the real identity (i.e., the SIM card number of the cell phone) RIDi. Then it refers to the record Table III to check if the PIDi sent by UEi and RIDi are one-to-one map. If so, it continues examining the UEi’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 RIDi6 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 UE7. Then the gateway responds the eNB with the real identities (RIDs) of candidates.

Step 4 Pair selection. The eNB chooses the proper candidate (supposing UEj ), 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 \( u = ga \) as a key hint. The communication request message \( (\text{PIDj} \parallel \text{PIDi} \parallel z \parallel \text{Pi} \parallel h(\bullet; x_j)) \) is then sent to the selected entity. Simultaneously, the eNB acknowledges the requesting UE the pseudo-identity PIDj and public key Xj of the transmitter, which means \( (\text{PIDi} \parallel \text{PIDj} \parallel Xj \parallel \text{Pi} \parallel h(\bullet; x_i)) \) being sent to UEi as a response.

Step 5 Data transmission. When receiving a communication request message

\[
\text{PIDj} \parallel \text{PIDi} \parallel z \parallel u \parallel \text{Pi} \parallel h(\bullet; x_i),
\]

the entity randomly selects \( b \in \mathbb{Z}_q^* \) and generates the communication key \( kc = zb = gcb \). With \( kc \) the entity encrypts the material \( M \) and gets \( M' = Enckc(M) \). Before sending the secure message \( M \), the entity signs the message by computing

\[
\sigma_2 = H_1(\text{PIDj} \parallel \text{PIDi} \parallel z \parallel u \parallel \text{Pi} \parallel h(\bullet; x_i))^{x_j}.
\]

The data is shaped in the format of Table V and sent to the intended UE. Note that signature 1 is finished in off-line stage by the SP. Timestamp Ts is applied to resist the replay attack.

Additionally, the key hint \( y = gb \) is computed for the receiver to generate the decryption key \( kc \). Rather than being sent to the receiver directly, the key hint is encrypted under the shared key \( ks \) with eNB, where

\[
\begin{align*}
\text{PIDi} &\parallel \text{PIDj} \parallel \text{Pi} \parallel \text{Encks}(y) \parallel v \parallel T_s \parallel h(\bullet; x_j) \end{align*}
\]

is sent 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, UEi extracts PIDj from the message. It compares PIDj with the pseudo-identity obtained from the eNB. If they don’t match, the packet is dropped. Otherwise, it performs signature verification by checking

\[
\text{e}'(Xj; H_1(\text{PIDj} \parallel \text{Pi} \parallel M' \parallel T_s \parallel 1)) = \text{e}'(2; g);
\]

If the equation holds, the data is considered to be sent by the entity with pseudo-identity PIDj. To decrypt the message \( M' \), UEi sends a key hint request message.
(PIDi∥ PIDj∥ Pi ∥ Ts ∥ h(•; xi)) 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 Encks(y) with ks = va and a response as (PIDi∥ PIDj∥ Pi ∥ y ∥ Ts ∥ Ti ∥ h(•; xi)) is delivered. Timestamp Ti 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, UEi can get communication key by computing kc = yc = gbc. 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

$$\hat{\epsilon}(X_0, H_1(P_i||M)) \equiv \hat{\epsilon}(\sigma_1, g).$$

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

$$\beta = (PIDi∥ PIDj∥ Pi ∥ M’ ∥ Ts ∥ 1 ∥ 2 ∥ h(•; xi));$$

to the eNB within the timestamp Ti’, which satisfies that Ti’ < Ti + ΔT (ΔT is the predefined time scale). The feedback beacon, 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 UEi. During the waiting time scale, if any feedback beacon arrives, the eNB first checks the validity of 1 by inspecting (5) as UEi had implemented. Note the payload M is not obtained by deciphering M’ as the eNB knows no information about the communication key kc. Instead it refers to the storage for the original data M with the corresponding portion index. If the signature 1 is invalid indeed, it is judged that the message is not originated 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 2 to ensure the fake message is sent by the entity with pseudo-identity PIDj;
2) The eNB refers to record Table III to disclose the real identity of PIDj and
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.

IX. SECURITY ANALYSIS

In this section, 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.

The proposed protocol ensures data confidentiality and integrity. During the process of transmission, the data is done with proper encryption (Encs(M)). Without gaining the key, the eavesdroppers can’t 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 gb and gc, still can’t derive the shared key gbc 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 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 1, the origin of the data is expected to be from SP, being considered as the authority service provider. Hence the data integrity and authority are guaranteed.

The proposed protocol ensures entity authentication. Entity authentication is implemented between the UE and eNB as well as 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 or not the real identity corresponds with the pseudo identity in the member record.

Generally, the authentication in D2D communication mode is implemented by the verification of the signature 2. Before sending the data to another device, the transmitter is assumed to make a signature on its pseudo identity and the data.

The proposed protocol is secure in conditional privacy preservation. In the SeDS protocol devices use pseudo identity, which is the secure one-way hash value of the real identity, for communication. It is computationally hard to identify the real identity of the entity. Note that the real identity of the UE or SP is disclosed to the trust authority eNB while 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 makes least efforts on sharing data with others. These free-riders may be punished by being not delivered information further more or excluded from the membership.

The proposed protocol ensures non-repudiation. The data sharing event is non-repudiation for both the sender and receiver. The signature 2 of the transmitter provides no opportunity for the entity to deny the transmitting event while it also offers the evidence of data sharing behavior, which may be proofed to be meritorious or malicious by the verification of signature 1. When a receiver verifies an invalid signature 1, it will send a feedback beacon to the eNB. By verifying the signature 1 from the evidence, the eNB first ensures that the message is indeed sent by the entity with pseudo identity PIDj. Then, by referring to the record table, the real identity 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. But there may be irrational attacker who only receives data but doesn’t intend to get the original information so 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.

The 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, non-repudiation 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 VI-C, it can be concluded that the proposed SeDS protocol is expected to provide available service to the users.

X. CONCLUSION

In this paper we have jointly studied key technologies, connectivity model, interface analysis, and cross layer design of D2D communication. The paper explains about how we can communicate using D2D communication technology without any data theft or any malfunctions. And also about the power consumption and interference that would take place in this process.

REFERENCES


