IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

SPECIAL SECTION ON RECENT ADVANCES IN CLOUD RADIO ACCESS NETWORKS

Received August 31, 2016, accepted September 28, 2016, date of publication October 20, 2016,
date of current version November 28, 2016.

Digital Object Identifier 10.1109/ACCESS.2016.2617207

Dynamic Trust Associations Over Socially-Aware D2D Technology: A Practical Implementation Perspective

ALEKSANDR OMETOV[1,3], EKATERINA OLSHANNIKOVA[1], PAVEL MASEK[2], THOMAS OLSSON[1], JIRI HOSEK[2], SERGEY ANDREEV[1], AND YEVGENI KOUCHERYAVY[1]

[1]Tampere University of Technology, 33720 Tampere, Finland
[2]Brno University of Technology, 601 90 Brno, Czech Republic
[3]Saint Petersburg National Research University of Information Technologies, Mechanics and Optics, 191002 Saint Petersburg, Russia

Corresponding author: J. Hosek (hosek@feec.vutbr.cz)

This work was supported in part by the Academy of Finland through the project Empowering Secure, Private, and Trusted Network-Assisted Device-to-Device Communication and the project Enhancing Knowledge Work and Co-Creation with Analysis of Weak Ties in Online Services, in part by the National Sustainability Program under Grant LO1401, and in part by the Foundation for Assistance to Small Innovative Enterprises within the Program UMNIK under Grant 8268GU2015. For the research, infrastructure of the SIX Center was used.

ABSTRACT Today, direct contacts between users are being facilitated by the network-assisted device-to-device (D2D) technology, which employs the omnipresent cellular infrastructure for the purposes of control to facilitate advanced mobile social applications. Together with its undisputed benefits, this novel type of connectivity creates new challenges in constructing meaningful proximity-based services with high levels of user adoption. They call for a comprehensive investigation of user sociality and trust factors jointly with the appropriate technology enablers for secure and trusted D2D communications, especially in the situations where cellular control is not available or reliable at all times. In this paper, we study the crucial aspects of social trust associations over proximity-based direct communications technology, with a primary focus on developing a comprehensive proof-of-concept implementation. Our recently developed prototype delivers rich functionality for dynamic management of security functions in proximate devices, whenever a new device joins a secure group of users or an existing one leaves it. To characterize the behavior of our implemented demonstrator, we evaluate its practical performance in terms of computation and transmission delays from the user perspective. In addition, we outline a research roadmap leveraging our technology-related findings to construct a holistic user perspective behind dynamic, social-aware, and trusted D2D applications and services.

INDEX TERMS Device-to-device communication, network security, cryptographic protocols, social network services, technology social factors.

I. INTRODUCTION AND BACKGROUND

In the networks of today, the mobile data volumes are increasing tremendously. To this end, the Visual Networking Index by Cisco claims that the traffic has already increased by more than 74% percent in 2015 [1]. Hence, it has been concluded that the networks as we know them presently are about to face a serious overload by 2025 [2] and thus novel connectivity enablers will become a must in future wireless systems [3]. As one of the attractive solutions for cellular network development, the network-assisted short-range communications is being established by offering the needed network capacity gains and at the same time facilitating the proliferation of proximity-based user applications and services. The main advantage of this emerging technology is to enable direct connectivity between users being in each other's proximity [4], [5]. This allows for such desirable features as better utilization of the unlicensed spectrum (in case of using WiFi as an underlying connectivity solution) as well as higher data rates in addition to lower energy consumption from both user and operator viewpoints [6]. The industry leaders are already proposing different solutions in this space [7], [8].

A. EMERGING PROXIMITY-ENABLED SOCIAL INTERACTION

From the perspective of mobile services, the volume of applications is indeed enormous, from the ubiquitous social networking [9] to the scenarios of National Security and Public Safety [10]. Today, application developers are already

experimenting with completely new forms of social interactions having the notion of ''wireless sense'' within the rapidly maturing proximity-aware ecosystem [11]. It is widely believed that sociality-based collective applications will occupy their unique niche and evolve in the nearest future. As the main trend for socially-aware direct connectivity, we envision an opportunity to communicate within a group of users being geographically close to each other. While current cellular networks can accommodate similar scenarios only partially, the network-assisted direct communications has the potential to offer additional benefits of lower latency, better battery efficiency, and higher user privacy.

Facilitated by the rapid development of network-assisted direct connectivity and respective proximate services, social user interactions may effectively bridge the physical and the virtual worlds. This novel communications paradigm is augmenting the capabilities of people to remain connected, as they can reach each other nearly everywhere. At the same time, due to the limited interactivity in computer-mediated communications (CMC), people face new challenges in e.g., maintaining existing relationships, gaining mutual understanding, and building trust with an unknown remote person [12]. As a glaring example, the lack of natural communication expressions in CMC creates trust and security concerns related to identity and access management (IAM) [13], [14]. Broadly, the field of IAM is targeting to offer security solutions enabling access to appropriate resources at certain times and for the relevant reasons. Consequently, there are more and more applications in need of simple and transparent IAM enablers. Here, proximity-based services are not an exception: public safety, corporate business, gaming, shopping, and multiple other sectors require efficient practices and technologies for managing user identities, privileges, access, and trust. However, traditional IAM solutions may lack full support in the dynamic and uncertain proximity-based service environments.

B. ENABLING TECHNOLOGY FOR PROXIMITY-BASED TRUST ASSOCIATIONS

The emerging device-to-device (D2D) communications technology has excellent potential to enable a wide range of proximate user applications and services. In this article, we aim at investigating novel approaches to facilitate simple, efficient, and trusted social interactions. The main thinking behind the corresponding security protocols is to enable a trusted social association framework (TSAF) allowing to construct (semi-)supervised D2D-based proximate communities. This inspires the group formation logic in our proposed proof-of-concept (PoC) prototype implementation described at length in this work. It is generally based on the concept of integrated centralized and distributed systems [15]. In this use-case, TSAF manages the access rights and resource allocation across group members and their devices according to the ''majority rule'' (a type of a threshold scheme), where all the users have equal voting rights to exclude or accept new members. This type of behavior is characteristic of small-scale user applications with reasonably low numbers of participants. Our PoC demonstration therefore seeks to shed light on the many challenges related to dynamic trust associations as well as helps understand the degrees of system scalability with larger user populations.

To resolve the above challenges, next-generation TSAF should become more intelligent than past conventional solutions by enabling centrally-assisted behavior for trusted community formation. Further research on voting taxonomy and social proximity networks is required to steer the development process and eventually make D2D-based group formation both feasible and reliable. In other words, we argue that the challenge of dynamic social trust associations needs to be addressed comprehensively for the future social proximity-based services to truly take off. This article outlines our respective research activities and summarizes the development of a complete PoC prototype implementation featuring a novel information security protocol suite for socially-aware D2D systems. Its main purpose is to enable secure data delivery for already communicating D2D users even in the cases of intermittent cellular connection. In particular, we assume that whenever several users have a link to the cellular system, they can establish and manage their own secure D2D network. Should the cellular connection become unavailable, our protocol suite allows for a set of existing users in the secure group to admit a previously unknown device or to exclude an existing one from the group [16]. Currently, group admission/exclusion can only be managed by the cellular network and our proposed formulations extend such functionality for the cases of partially unreliable cellular connection [17].

C. D2D CONNECTIVITY IN MOBILE NETWORKS

As discussed at length in our preliminary work on the subject [18], the lack of bandwidth becomes one of the most significant factors faced by the mobile network operators. Therefore, the anticipated applications for proximity-based communications are many [4], including proximate call offloading (both video and audio), multimedia content distribution, and proximate gaming, among others [10]. Network community is actively discussing new use-cases in this context. For example, wearable communications is about to open a whole new variety of applications. Wearable wireless devices (fitness bands, smart-watches, and eyewear) naturally exploit direct channels for their operation. Moreover, it is believed that D2D connectivity will support various machine-type communications (MTC) devices in their information sharing capabilities [19]. Furthermore, the MTC domain could additionally benefit from enabling vehicular communications over D2D [20], [21], smart-home automation use-cases [22], and by advancing the concept of the Internet of Things in general.

Today's wireless technology landscape offers a number of alternative solutions to be used as enablers for D2D operation. The ''classical'' radio technologies, such as IEEE 802.11 (WiFi) and IEEE 802.15.4 (BLE, ZigBee) are

operating in the unlicensed bands. The most attractive one is, indeed, WiFi mainly due to its lower transfer delay and higher throughput. Relatively recently, the WiFi-Direct was introduced [5] as an enhanced technology for proximate communications over WiFi. It facilitates direct infrastructureless connectivity and offers a possibility for multiple simultaneous group connections.

On the other hand, some believe that the licensed spectrum connectivity is a solution for efficient direct communications, which is referred to as LTE-Direct operating under the full control of the cellular infrastructure. Unfortunately, due to the complexity of this technology as well as slow standardization process, the resulting deployment is not expected any time soon [23]. Even if it is completed within an acceptable time frame, the interference and power management aspects would produce multiple challenges for practical D2D applications. In case of WiFi-Direct however, the built-in stock WiFi transceivers can be utilized and therefore our main focus in this work remains on implementing direct connectivity over the unlicensed bands. Based on the above pros and cons, we employ the WiFi-equipped devices in our corresponding trial of socially-aware D2D communications.

The rest of this text is organized as follows. In Section II, a detailed summary of our proposed security framework together with the necessary modifications to the deployed 3GPP LTE network are offered. Our implemented practical scenario accounting for all the communication phases is outlined in Section III. Performance evaluation follows in Section IV. In Section V, we discuss existing solutions for trust management and ways to utilize them for socially-aware D2D technology. Further, we also elaborate on how to improve the proposed PoC application based on the social D2D paradigm. The last section concludes this work.

II. IMPLEMENTING SECURE D2D MESSAGING

In order to conclusively trial the proposed theoretical security-centric framework for D2D connectivity, which was recently outlined in [15], we aim to develop a prototype application within the most widely used Android platform. The constructed application combines features of a secure messenger based on the proposed information security primitives. Before proceeding further, we familiarize the reader with our envisioned network architecture.

A. TEST 3GPP LTE DEPLOYMENT

Our prototype was developed within the live 3GPP LTE deployment (see Fig. 1), which is located at Brno University of Technology (BUT), Czech Republic. The subject LTE core is a fully-operational cellular infrastructure, while the full LTE testbed is utilized for the purposes of research and education. Its essential modules are listed in Table 1.

The described experimental 3GPP LTE (Release 10) network, (see Fig. 1), represents a complete commercial-grade implementation of all the crucial subsystems composing contemporary fourth-generation mobile networks. The radio access network (RAN) comprises two eNodeBs

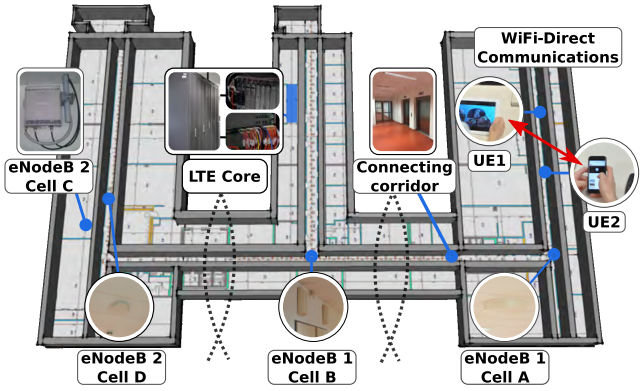


FIGURE 1. Test 3GPP LTE deployment: structure and main modules.

TABLE 1. Main components of our experimental 3GPP LTE deployment.

Core units	Components	Description
EPC	UGW (SGW, PGW)	Fully redundant 10 Gbps links.
	MME	Interface mirroring for probe-based analysis.
	HSS	
IMS	IMS-HSS	IMS core + RCS,
	ENUM/DNS	Enables VoLTE,
	S-CSCF/MRFC	Public Safety Answering Point,
	P-CSCF/A-SBC	Additional HSS,
	MRFP	Full redundancy.

and one Home eNodeB. The indoor eNodeBs are divided into two components: (i) the baseband unit (BBU) and (ii) the remote radio unit (RRU). As a eNodeB unit, Huawei DBS3900 (an indoor macro base station) is utilized. It features (i) a BBU3900 (management logic for eNodeB e.g., mobility management and modulation techniques in base band), and (ii) the RRU (modulation of used frequency). In more detail, the eNodeB 1 includes two cells (Cell A and Cell B) operating in the band 17 (originally, the AT&T band in US, 700 MHz). The eNodeB 2 manages three cells (sectors) working on separate frequencies 700 MHz, 2600 MHz (these two are indoor pico-cells), and outdoor 1800 MHz (not shown in the figure). Next, the WiFi access points (APs) are incorporated together with the LTE cells as part of the integrated network. The APs operate in the ISM bands (2.4 GHz and 5 GHz) and provide with a possibility to utilize packet-switched data services, such as VoIP or VoLTE.

For the purposes of testing the emerging technologies, the evolved packet core (EPC) enables access to the RAN part of the LTE network for up to 100,000 terminals (end-users). Following the recommendations released by the Czech telecommunication office, the TX power for indoor cells is set to 1 W (30 dBm) and the provided data rates are up to 33 Mbps in the downlink and up to 13 Mbps in the uplink channel. On top of that, the Quality of Service (QoS) and Quality of Experience (QoE) techniques are implemented for the served terminals. This full-featured LTE testbed accommodates our research and education needs by allowing full access to the experimental cellular network. It is used in this work to

obtain deeper understanding of system operation principles as well as to open the door to rapid and efficient prototyping of new wireless technology, including D2D communications and data offloading mechanisms.

While working on our intended trial setup, several modifications had to be made to the given LTE network – primarily regarding the firewall policies and default configuration of the IP Multimedia System (IMS) component. As our initial step, we developed and implemented an additional server (physically located in the IMS), which provides the IP-based data communications between the user terminals. Moreover, said server is responsible for (i) the security certificate generation and (ii) the distribution of generated certificates (to offer a possibility of secure data transmission over the mentioned RAN parts of the system, the WiFi and the LTE RANs).

B. MODIFYING D2D-SPECIFIC MODULES

Having an opportunity to (re)configure the network setup, we were able to enable direct connectivity between the devices connected to the RAN part of said LTE network. The various communications technologies (i.e., LTE and WiFi) were utilized jointly without the need for implementation of e.g, separate infrastructure hot-spots. In commercial LTE systems, direct communications between the devices within the RAN is limited by the telecom operators. This leads us to the situation when the connected devices can establish their data transmission sessions even if they are not inside the cellular network coverage.

Importantly, when the user devices are not under the network coverage i.e., the managing entity is not available, it makes the establishment of secure connections complicated. In the modern wireless networks, the IPv4 protocol is used commonly and each connected device possesses a unique IP address for the purposes of its data connectivity. This address is provided by the network (cellular infrastructure) and in most situations is dynamic over time. In case of out-of-coverage communications, new policies and routing protocols should be constructed and implemented, since the default firewall configurations in the deployed LTE networks may restrict the possibility to establish direct access from one device to another. As a result, this might limit the potential opportunities provided by the D2D technology. In connection to the above, we have implemented a new set of firewall policies, which allow for direct communications between the connected cellular network users and the mentioned server (located in the IMS), see Fig. 2.

C. IMPLEMENTING A SECURE D2D FRAMEWORK

In a nutshell, the considered D2D system is built upon the advanced security protocols described in [24]. It is intended to be managed by the server operating inside the LTE infrastructure as well as previously described in our past work [25]. To this end, the mobile users may establish and utilize a direct link only if they have a reliable connection to the D2D server that is responsible for the key and connection management [26].

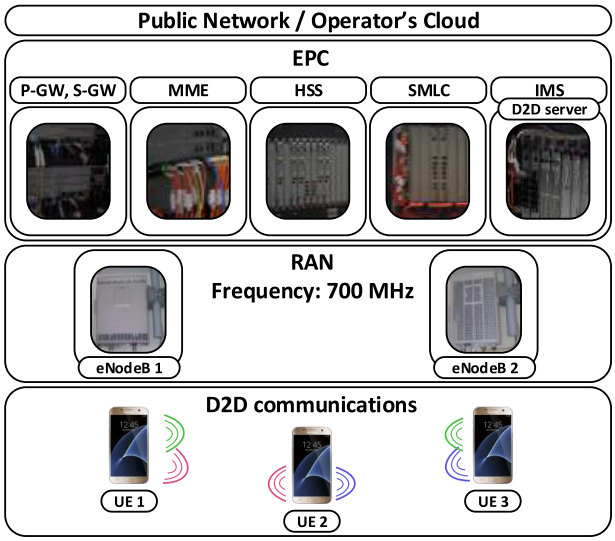


FIGURE 2. Prototype implementation of a D2D system.

In the networks of today, the Public Key Infrastructure (PKI) within the operator's network is conventionally responsible for the orchestration of the secure communications [27]. However, this technology can only be utilized while having a reliable connection to the infrastructure network and thus many applications cannot be enabled if at least one user leaves the network coverage. The necessary step to maintain the direct connectivity operational is to employ the distributed solutions [28]. They bring along completely new information security challenges related to distributed discovery, authentication, trust, and privacy maintenance, which are traditionally handled by the network operator.

Contemporary systems do not provide efficient enablers for cellular-assisted distributed mobile networking if there is no connection to the server. The real-world topology dynamics and unpredictable changes in trust relationships between the users should thus be tracked back and reported to the network as soon as any of the involved users reach cellular coverage. This is why existing solutions related to the conventional ad-hoc networks are not applicable in the D2D context, as it was demonstrated by our preliminary work in [15]. In what follows, we focus on two main operating modes of the proposed protocol suite: *reliable and unreliable cellular connectivity*.

In this work, we concentrate on typical cellular-assisted secure D2D group functioning and the corresponding operating states are summarized in Table 2. The developed solution builds on top of the 3GPP model and allows to support communications in the situations with no stable cellular connectivity. Importantly, device discovery is assumed to be handled by the cellular service. Therefore, we consider that the cellular system serves as the trusted certificate authority (CA) for the devices involved into proximity-based communications. Each of them has a unique ID and a certificate signed by the CA whenever this device associates with the cellular

network initially. This certificate is utilized for secure group establishment by means of the user validation.

The only procedure of our proposed framework that requires stable connectivity to the server is secure group (coalition) initialization. First, the involved mobile devices receive their certificates with the corresponding secret and public keys. Further, this set is utilized to establish secure direct communications with each other. When one of the users is willing to create a secure group with its neighbor, a corresponding request containing the IDs of the future group participants is delivered to the corresponding server in the network. A polling procedure is then triggered by the CA to ensure that the subject users are willing to join the group. After a confirmation has been received, the CA generates a group certificate and a group secret based on the Lagrange polynomials technique, as it is detailed in [15]. After these initial steps, secure direct communications may continue over any conventional IP network.

We emphasize that in the cases of unreliable cellular connection, secure associations inside the group enable D2D communications to be fully operational. Accordingly, the clients do not transfer their data through the server but instead communicate directly. Further, in our proposed framework, the D2D users in the coalition may take advantage of community-oriented voting whenever it is required to include another client into the group or to exclude an existing user from it. The client devices may hence execute a voting procedure in two distinct cases: when all of them have a connection to the infrastructure and thus to the CA or, otherwise, when at least one of them does not have it.

If a cellular connection is available, the operation of joining or leaving the secure group will be regulated by the server. According to the voting results that involve the existing users, the server generates and distributes new group certificates for the modified coalition. Conversely, in case when the infrastructure is inaccessible to at least a certain share of the devices, these clients may vote inside their coalition directly. Such an operation mode might be enabled by means of indirect group secret reconstruction based on a preset threshold value that reflects the required number of users to be grouped together while recovering the secret. Finally, the members of thus updated coalition could recreate a new share to include another device or use their shares to exclude an unwanted user.

Clearly, share recovery coupled with a polling mechanism needs extra computing energy as well as additional exchange in signaling messages as compared to the conventional infrastructure-based operation. On the other hand, the proposed framework offers higher QoS and connectivity experience for the group members. In the following section, we introduce our designed framework and focus on the proposed protocol details.

III. CONSIDERED SCENARIO FOR SECURE D2D

In this section, our prototype implementation of socially-aware D2D setup is detailed. We additionally discuss the proposed framework operation that is also supported by the summary live-trial video in [29].

Within this trial implementation, we have deployed a Linux-based server running a Python service into the 3GPP LTE network with a D2D server, see Fig. 3. In this sense, the server is acting as the CA in addition to managing the authentication and the logical IP association procedures. The Easy-RSA coupled with the OpenVPN tools were utilized for generating and updating the certificates. We employed four Samsung Galaxy S4 phones running non-rooted firmware version 4.4.2 for the purposes of this demo. A characteristic scenario for the use of our developed prototype is described in what follows.

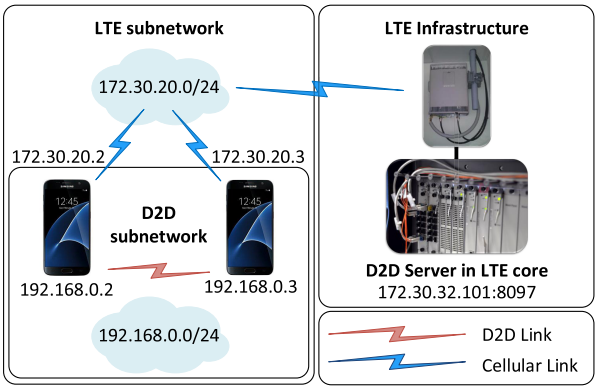


FIGURE 3. Target scenario for secure D2D communications.

A. TARGET APPLICATION SETUP

Logically, we begin our description with the group initialization phase. In our example, three out of four devices are connected to the cellular network. Their users are launching the application that in its turn is generating initial public and secret keys to enable preliminary secure communications. The CA certificate is embedded into the application. Further, each of the devices establishes a connection to the CA via an LTE link using the TCP sockets, where all the initial signaling is signed by the CA's public key. Next, the user's public key is sent to the CA and associated with the user's unique ID – *Username@PublicIP*. Here, *PublicIP* stands for the IP allocated to the mobile device within the cellular network. Further, the CA generates a certificate for each user and signs it with the *root* certificate. The server also delivers user certificates and secrets to the corresponding owners, while the public keys are forwarded to other users upon request. As a result, direct D2D connectivity on top of the cellular network becomes feasible.

B. COALITION INITIALIZATION

The second phase corresponds to the coalition creation (see Table 2). In order to successfully execute the initialization phase, the server requires the knowledge of the clients in proximity that are willing to connect. This information may be based on geolocation, sensing the environment, or cellular assistance techniques. Assume that one out of three clients

TABLE 2. Modes of D2D system operation and our proposed procedures.

States	Not in coalition	In coalition
Not in coverage	① Join	② Vote; Leave
In coverage	③ Initialize; Join	④ Initialize; Vote; Leave

is interested in creating a secure coalition. Accordingly, this user device sends a request to the server with regards to its proximate clients and receives a reply with their IDs. The initiating user can then select which of these potential partners will be invited into the future coalition. After the users are chosen, the initiating device sends this list back to the server.

Further, polling/voting procedure is triggered at the server side, when each of the client devices from the list is prompted as to whether it is willing to join the coalition. The responses are reported back to the server, which is expecting the replies within a given period of time in order to provide operational consistency. If the reply is not received on time, it is treated as negative. In essence, a group secret is generated based on the Lagrange polynomial sequence [30], and a threshold value for adding and removing users to/from the group is set according to the security policy of the operator/user, whereas each user certificate is being signed by the secure group certificate. User certificates are updated on the user side over a secure infrastructure connection.

C. VOTING IN EXISTING COALITION

1) RELIABLE INFRASTRUCTURE CONNECTION

At the next stage, we outline the user adding procedure in case of a reliable connection to the server, which may occur in case ④. Here, one of the user devices included into the existing coalition is requesting the server to add a device that is not a part of it yet. The request contains the group name and the ID of the device to be included. The CA is further triggering the polling procedure and collects the replies. If a reply is not received within the preset time period – the answer is assumed to be negative. After the decision is reached and in case it is positive, the certificates are redistributed correspondingly as well as the coalition secret is updated. Exclusion of a user is performed similarly. Additionally, a user can leave the coalition on its own, by removing the group certificate and/or reporting on this fact to the server.

2) UNRELIABLE INFRASTRUCTURE CONNECTION

Compared to the infrastructure case, adding and removing users without a reliable network connection becomes a more involved task i.e., in modes ① and ③. At first, the users have to execute the routing protocol allowing for message exchange via an ad-hoc-like network. Having the knowledge that the users are already in proximity, that is, belong to the same subnetwork, the protocol forces user devices to re-associate their IP addresses utilized when connected to the server. Unfortunately, Android platform does not natively support such functionality [31]. Therefore, we have implemented it using *our own solution*: given that the unique device ID includes the IP address together with the user name, where the former is used in the cellular network and cannot be changed manually by the user, the application can only interact with the IP on the WiFi interface.

Since simple distributed routing is established, we focus further on the security protocol implementation in cases of unreliable cellular connectivity. Hence, we briefly describe the coalition joining procedure in case when the CA is unreachable. Our only requirement for supporting this case is for any new user to reside within the same physical wireless network as the rest of the existing users in the coalition. If this requirement is satisfied, we can imply that all of the coalition users are in proximity and can communicate with each other. Therefore, a new user should distribute its public key (previously signed by the CA) among all the coalition partners at first.

If the above procedure was successful, the user may then be invited to join the coalition after a local polling triggered by one of the trusted devices inside the coalition. The inviting device is collecting the responses from the rest of the participants. If the number of acceptance replies is higher than a certain threshold value, the group launches the joining protocol for the purposes of generating new shares. In essence, it is a modified secret recovery scheme based on the Lagrange polynomial sequence i.e., if k out of n devices assemble together, they can indirectly reconstruct the polynomial and obtain another *point* on the curve for the newly-joining user.

The user exclusion is performed in a similar manner i.e., a set of users may group together aiming to remove one from the coalition. They cannot affect the share of the unwanted user, and instead regenerate the coefficients for their shares, that is, change the behavior of the polynomial in agreement between all of them and thus save the original secret of the group. Importantly, when a user is included to and excluded from the secure group, the *actual* participants store the chain of the coalition modifications that is signed and redistributed after each event. Based on this chain, the server can later receive a complete and trustworthy update on the events that have occurred to the coalition while it has remained unreachable. The main idea here is to keep track of the certificate updates at the group side. Finally, any device can leave the coalition at an arbitrary moment of time by removing its own share.

IV. USABILITY EVALUATION OF OUR POC PROTOTYPE

In this section, we analyze how usable the proposed socially-aware D2D system could be if we would increase the provided level of strong cryptography for our PoC implementation. Information security specialists are now recommending the use of at least 1024 bits key size and this is taken as the main parameter of our evaluation here [32], [33]. This size is also expected to grow further for up to 3072 bits by 2030. Therefore, we aim to analyze the effects of such an increase on our proposed solution. We note that the most important factor for the mobile device users is the application response

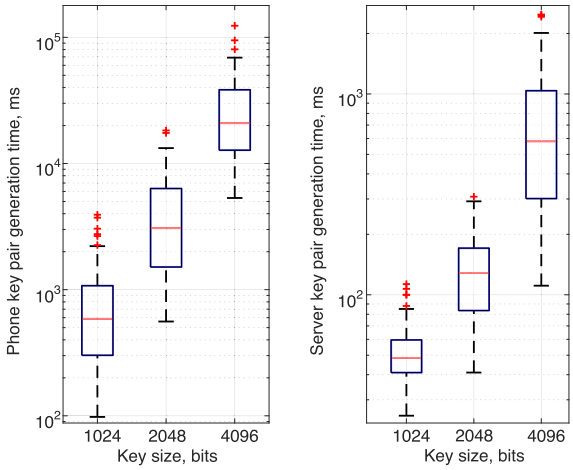


FIGURE 4. Key pair generation time: server and user equipment.

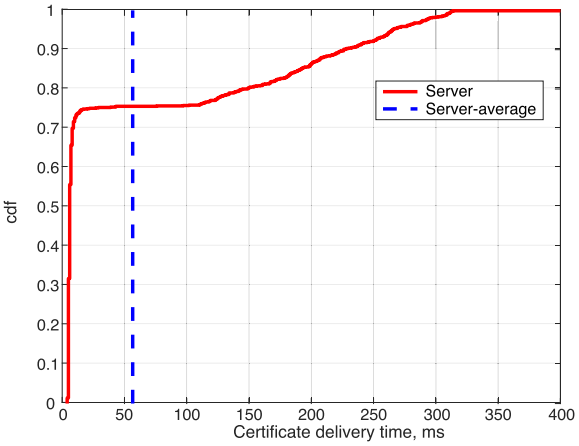
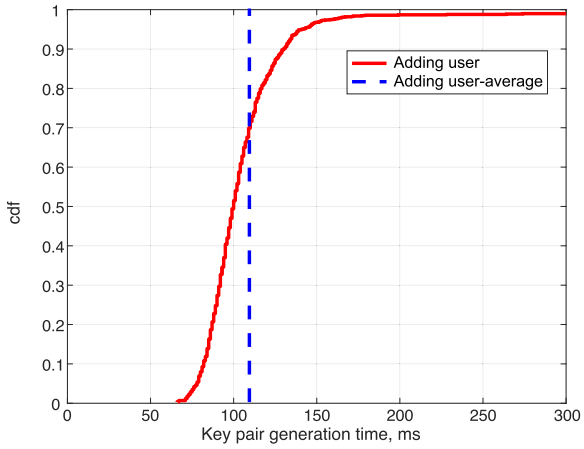
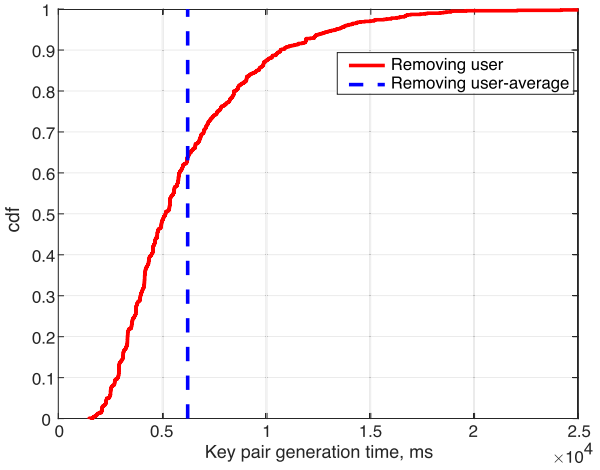


FIGURE 5. Certificate delivery time (infrastructure mode).



(a) Add user procedure



(b) Remove user procedure

FIGURE 6. Operation time in the ad-hoc mode. (a) Add user procedure. (b) Remove user procedure.

time i.e., the delay. Hence, we consider the certificates, keys, and shares generation time observed by the user for both cases of reliable and unreliable connectivity to the infrastructure.

Based on the protocol operation model and prior to actual direct communications, the users have to obtain a certificate containing a secret and a public key. On the one hand, it is recommended to be handled by the corresponding server inside the cellular infrastructure and delivered securely. On the other hand, this pair of keys could be generated at the user side if the network connection does not provide with the required reliability. Accordingly, Fig. 4 offers a summary of the corresponding execution times for the key generation cases thus comparing the capabilities of a modern mobile device and the average server. As we can see, the server is operating up to 30 times faster than the mobile device for the case of 1024 bits key size. By increasing this value to 4096 bits, the advantage grows to around 100 times. We therefore conclude that the key generation time of 100 seconds is unacceptable from the user's viewpoint. However, taking into consideration the key-length recommendations of today, 3 seconds may represent a feasible initial setup time.

Analyzing our PoC implementation, we model a scenario with four devices that have an opportunity to automatically accept or deny the addition/exclusion requests of the group members during the voting procedure (i.e., the PPDR case [10]). This application was modeled mainly to evaluate the network performance without any human-dependent delays and the corresponding results are given in Fig. 5. We decided to investigate here a more secure operation regime by utilizing 2048 bits keys. The provided plots include the time needed to establish a connection, conduct transmission, and perform data processing. These phases are executed independently of the user behavior and may thus become a useful reference point for future system implementations or improvements.

As another important step of our analysis, we consider the operation of a purely ad-hoc mode i.e., when the connection to the cellular infrastructure is not reliable. The respective results are presented in Fig. 6. Here, the procedure of the share generation for a new user takes approximately the same time as compared to the server-driven operation. The observed

fluctuations are because of the unpredictable nature of the underlying random access mechanism of IEEE 802.11. It is worth noting that the time consumed by the system while excluding the user from an existing group may constitute up to 5 seconds even for smaller numbers of devices, which can directly affect the communications consistency.

Interestingly, the "remove user procedure" takes more time than the "add user procedure", as evidenced by Fig. 6. The main reason why excluding a user consumes more time is because the corresponding protocol operates in the ad-hoc mode. In particular, to add a new device without the infrastructure connection, the trusted clients should cooperate and generate *only one* new share for this user to join. However, when excluding a device, the clients in the coalition should regenerate all of their own shares, which results in higher signaling and computation overheads.

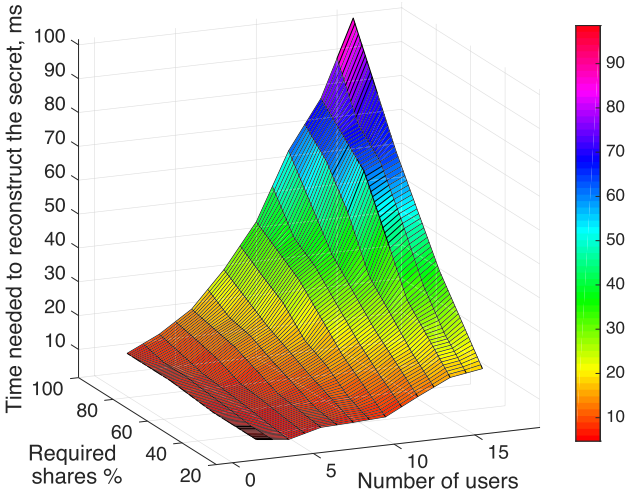


FIGURE 7. Comparing the time to reconstruct a secret.

Finally, our modified model was tested by evaluating the time required for the secret reconstruction on a contemporary smart phone. We thus considered the Samsung Galaxy S4 device and the respective results are visualized in Fig. 7. On the vertical axis, the time needed to reconstruct the secret is displayed by varying both the threshold value (the number of users in the coalition that have to be grouped) and the maximum number of users in the same group. Generally, the computation complexity of executing the information security primitives grows exponentially due to the properties of the Lagrange polynomial function. Moreover, adding another user to participate in this procedure brings at least 2 handshakes from the communications point of view. As the plot demonstrates, the proposed protocol requires less than 100 ms for the new share (point) generation for both joining and excluding procedures.

In conclusion, we state that the developed protocol and the accompanying prototype implementation are suitable for utilization from both the user and the technology perspectives, where the main conclusions are summarized in Table 3.

TABLE 3. Summary of the PoC usability evaluation.

Feature	Conclusion
Key size	Increasing the key size from recommended 1024 to 4096 bits brings a slight issue with the computation complexity on the mobile device side while utilizing 2048 bits is still acceptable (Fig. 4).
Initialization phase	In case when devices automatically confirm new joining users, the average certificate generation and delivery time takes less than 60 ms in the infrastructure mode (Fig. 5).
Unreliable cellular connectivity	While operating in the pure ad-hoc mode, adding a new user takes less than 120 ms on average, whereas excluding a user may consume up to 5 s in the worst case (Fig. 6).
Secret reconstruction	Time needed to reconstruct the secret grows exponentially, as the proportion of users that participate in the voting increases. Similar behavior is observed when increasing the overall number of users in the group (Fig. 7).

V. SOCIAL TRUST ASSOCIATIONS: RESEARCH ROADMAP

In the course of our protocol and prototype development, we reviewed some of the most important trust challenges in dynamic proximity-based communications systems facilitated by the network-assisted D2D connectivity that is further discussed in this section. While working on the integration phase, our group solved a number of problems with respect to the 3GPP LTE system operation, networking, and routing on the device side in addition to many smaller issues related to enforcing security on Android platforms. In particular, we had to (i) update the effective LTE firewall policies, (ii) design and implement a custom routing protocol (LTE to WiFi), and (iii) construct a modified Shamir Secret Sharing scheme together with all of the required modular algebra primitives, tailored specifically for Android.

As a result, the discussed numerical findings may become an important consideration for resource-constrained devices (e.g., wearables), as today's limited computing power of those may have difficulty in satisfying the requirements of the security primitives utilized by our current solution. Improving the considered constructs with the methods of lightweight cryptography is therefore an ongoing direction of our work. More broadly, the proposed socially-aware D2D PoC framework is only a first research step on social trust associations in proximity-based services. The goal of the rest of this section is to provide with a vision on how the knowledge from multiple disciplines could be integrated to shift the social group formation onto the semantic level. We believe that it will bring useful insights not only for our planned future research, but also benefit the broad D2D-focused community.

The problem of trust has puzzled researchers in various contexts and thus multiple disciplines have studied trust relationships since 1950s, which resulted in a very large number of contributions [34]–[37]. We emphasize that 'trust' is an abstract, multi-faceted phenomenon that is often used interchangeably with the related concepts, such as credibility, reliability, or confidence [38]. Therefore, there are many meanings and interpretations of trust and the ways of reaching

it. The following definition has been given in [39], which we generally agree with: *Trust is the extent to which one party is willing to participate in a given action with a given partner, considering the risks and incentives involved.*

In relatively short-term and highly dynamic proximity-based communications, it is challenging to develop trusted relationships due to depersonalization effects, which are discussed in [40]. Describing this phenomenon in terms of socio-psychological aspects of CMC, we reveal the fact that wireless connectivity tends to be impersonal. This results in decreasing the risks of social isolation as, typically, in virtual environments it is hard to track the individual behavior while user identity could be hidden. However, communications system may obtain this important knowledge over time by e.g., utilizing the many machine learning methods, including artificial neural networks [41]. The system could also track various aspects of personal digital activities, interactions, and interconnections with other people and thus be able to estimate the level of trust. For instance, rich information from social networks, as well as friend and contact lists together with recent social connections could be employed to predict the objective trustworthiness. Along these lines, the structure of dynamic social groups is studied across the disciplines of social network analysis [42], [43].

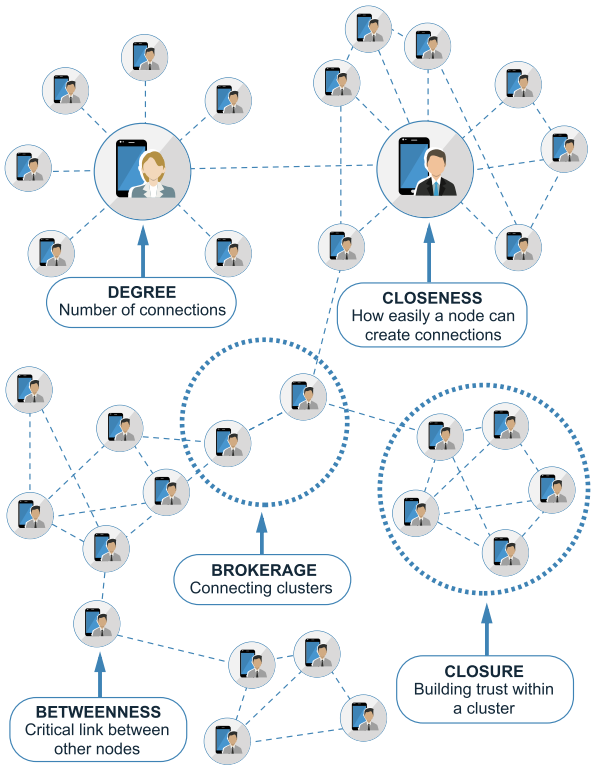


FIGURE 8. Structure of proximate social networks.

Categorization of the network elements allows us to identify strong social connections in the real world (see Fig. 8). For instance, we highlight two elements in the social networking structure that influence the dynamic and trustful group formation – *brokerage* and *closure* [44]. These categories reflect the idea of developing strong ties within the group of people in order to achieve beneficial and trusted relationships as well as to connect the social clusters. Further, *degree*, *closeness*, and *betweenness* are the essential characteristics of an individual node.

Here, *degree* is the number of connections that a single node has. For instance, in case of D2D communications, the more social connections an individual has (e.g., friend list in Facebook, connections on LinkedIn, etc.), the higher would be the potential for this user to build reliable relationships within a social cluster in the proximity-based network. Further, mapping the existing links (trusted relationships) across individuals enables identification of potential new links and demonstrates that even people who do not know each other personally often have a 2nd or 3rd degree connection. Therefore, the notion of friend-of-a-friend could be used as a predictor of new trusted relationships and then employed in future proximate services.

The evaluation of *closeness* could reveal how easily an individual can build connections with others. In both physical and virtual worlds, a simple way for people to connect is to be in close proximity or have mutual acquaintances. The shorter the distance between the nodes is, the smaller the effort required to initiate communications would be. Additionally, a person could become a trust-builder between strangers, which is often named *betweenness*, thus becoming an important consideration that identifies critical links among people. This also gives the individual a possibility to block or enable access to others users. In terms of assisted D2D communications, such a node could have a high "value" for a proximate service to build new social clusters as well as steer interaction and improve the levels of trust between neighbors.

In addition to the social network analysis, the device itself could provide meaningful data that will lead to trusted social relationships between nodes. For instance, the interaction within a group of people could be initiated based on the similarity of content stored in their devices (e.g., individuals prefer similar data, applications, or services). In this case, ties and, possibly, improved trustworthiness could be developed based on the likelihood of user content. In summary, the application of neural computations as well as deeper understanding of the underlying social network structure could be employed in proximity-based environments to automate dynamic social trust associations and the corresponding resource management. Real-time analysis of the discussed concepts as well as consideration of the desired user content in personal devices could facilitate future TSAF and open new opportunities for secure and trusted socially-aware D2D applications.

VI. CONCLUSIONS AND LESSONS LEARNED

In this work, we reviewed some of the important trust challenges in dynamic proximity-based communications systems facilitated by the network-assisted D2D connectivity. To this end, we developed and evaluated a novel PoC framework

that enables a group of neighboring devices that have their D2D connections controlled and maintained by the cellular network to establish dynamic trust associations. The implemented functionality has been described at length in this article and includes the capabilities of adding new users to a secure coalition as well as excluding the existing ones from it even in the cases where reliable cellular network connection may turn out to be unavailable. Based on this PoC implementation, we performed a more detailed performance evaluation of the key generation, distribution, user addition, and removal functionalities from the time–complexity perspective. These results are novel in the field as they provide a first-hand report on the practical operation and limitations of secure network-assisted D2D connectivity for realistic system parameters.

In conclusion, our results offer a comprehensive baseline to build next-generation socially-aware D2D applications and services, as well as leverage the full potential of personal user interactions in the emerging proximity-based ecosystem. Accordingly, in this article we have also outlined a feasible research agenda that incorporates the notions of sociality and trust, as well as takes advantage of the state-of-the-art D2D technology, to empower novel opportunities for groups of humans in proximity. Ultimately, our research has the potential to bridge the current divide between the virtual and the physical communities thus opening the door to a plethora of novel applications that benefit from the recent technology progress across both worlds. For example, these could be smart and serendipitous services that have the knowledge of user's social network structure to offer new possibilities for trusted friend-of-a-friend types of connectivity for people in proximity, thus enriching their business and leisure experience.

REFERENCES

[1] *Cisco Visual Networking Index: Global Mobile Data Traffic Forecast*. (Feb. 2016). [Online]. Available: http://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/mobile-white-paper-c11-520862.html

[2] Ericsson AB. (Feb. 2016). *Ericsson Mobility Report: On the Pulse of the Networked Society*. [Online]. Available: http://www.ericsson.com/mobility-report

[3] S. P. Yeh, S. Talwar, G. Wu, N. Himayat, and K. Johnsson, "Capacity and coverage enhancement in heterogeneous networks," *IEEE Wireless Commun.*, vol. 18, no. 3, pp. 32–38, Jun. 2011.

[4] G. Fodor, S. Sorrentino, and S. Sultana, "Network assisted device-to-device communications: Use cases, design approaches, and performance aspects," in *Smart Device to Smart Device Communication*. Switzerland: Springer, 2014, pp. 135–163.

[5] F. H. P. Fitzek, M. Katz, and Q. Zhang, "Cellular controlled short-range communication for cooperative P2P networking," *Wireless Pers. Commun.*, vol. 48, no. 1, pp. 141–155, Jan. 2009.

[6] H. Luo, R. Ramjee, P. Sinha, L. E. Li, and S. Lu, "UCAN: a unified cellular and ad-hoc network architecture," in *Proc. 9th Annu. Int. Conf. Mobile Comput. Netw.*, 2003, pp. 353–367.

[7] K. Doppler, M. Rinne, P. Janis, C. Ribeiro, and K. Hugl, "Device-to-device communications; functional prospects for LTE-advanced networks," in *Proc. IEEE Int. Conf. Commun. Workshops (ICC)*, Jun. 2009, pp. 1–6.

[8] G. Baldini, S. Karanasios, D. Allen, and F. Vergari, "Survey of wireless communication technologies for public safety," *IEEE Commun. Surveys Tut.*, vol. 16, no. 2, pp. 619–641, 2nd Quart., 2014.

[9] E. Cho, S. A. Myers, and J. Leskovec, "Friendship and mobility: User movement in location-based social networks," in *Proc. 17th ACM SIGKDD Int. Conf. Knowl. Discovery Data Mining*, 2011, pp. 1082–1090.

[10] G. Fodor, S. Parkvall, S. Sorrentino, P. Wallentin, Q. Lu, and N. Brahmi, "Device-to-device communications for national security and public safety," *IEEE Access*, vol. 2, pp. 1510–1520, Dec. 2014.

[11] M. S. Corson, R. Laroia, J. Li, V. Park, T. Richardson, and G. Tsirtsis, "Toward proximity-aware Internetworking," *IEEE Wireless Commun.*, vol. 17, no. 6, pp. 26–33, Dec. 2010.

[12] C. Thurlow, L. Lengel, and A. Tomic, *Computer Mediated Communication*. Thousand Oaks, CA, USA: SAGE, 2004.

[13] M. Benantar, *Access Control Systems: Security, Identity Manage. Trust Models*. Springer Science & Business Media, 2006.

[14] L. Militano, A. Orsino, G. Araniti, M. Nitti, L. Atzori, and A. Iera, "Trust-based and social-aware coalition formation game for multihop data uploading in 5G systems," *Comput. Netw.*, pp. 1–11, Aug. 2016.

[15] A. Ometov, K. Zhidanov, S. Bezzateev, R. Florea, S. Andreev, and Y. Koucheryavy, "Securing network-assisted direct communication: The case of unreliable cellular connectivity," in *Proc. IEEE 14th Int. Conf. Trust, Secur. Privacy Comput. Commun. (TrustCom)*, vol. 1. Aug. 2015, pp. 826–833.

[16] L. Militano, A. Orsino, G. Araniti, A. Molinaro, and A. Iera, "Overlapping coalitions for D2D-supported data uploading in LTE-A systems," in *Proc. IEEE 26th Annu. Int. Symp. Pers., Indoor, Mobile Radio Commun. (PIMRC)*, Aug./Sep. 2015, pp. 1526–1530.

[17] G. Fodor *et al.*, "Design aspects of network assisted device-to-device communications," *IEEE Commun. Mag.*, vol. 50, no. 3, pp. 170–177, Mar. 2012.

[18] A. Ometov, P. Masek, J. Urama, J. Hosek, S. Andreev, and Y. Koucheryavy, "Implementing secure network-assisted D2D framework in live 3GPP LTE deployment," in *Proc. IEEE Int. Conf. Commun.Workshops (ICC)*, May 2016, pp. 749–754.

[19] A. Orsino, G. Araniti, L. Militano, J. Alonso-Zarate, A. Molinaro, and A. Iera, "Energy efficient IoT data collection in smart cities exploiting D2D communications," *Sensors*, vol. 16, no. 6, p. 836, 2016.

[20] C. Campolo, A. Vinel, A. Molinaro, and Y. Koucheryavy, "Modeling broadcasting in IEEE 802.11p/WAVE vehicular networks," *IEEE Commun. Lett.*, vol. 15, no. 2, pp. 199–201, Feb. 2011.

[21] G. Piro, A. Orsino, C. Campolo, G. Araniti, G. Boggia, and A. Molinaro, "D2D in LTE vehicular networking: System model and upper bound performance," in *Proc. 7th Int. Congr. Ultra Modern Telecommun. Control Syst. Workshops (ICUMT)*, 2015, pp. 281–286.

[22] J. Hosek, P. Masek, D. Kovac, M. Ries, and F. Kröpfl, "IP home gateway as universal multi-purpose enabler for smart home services," *E & I Elektrotechnik Informationstechnik*, vol. 131, no. 4–5, pp. 123–128, 2014.

[23] LTE Direct, "The case for device-to-device proximate discovery," Qualcomm Research, San Diego, CA, USA, Tech. Rep. 92121, 2013.

[24] *Universal Mobile Telecommunications System (UMTS); LTE; Proximity-Based Services (ProSe); Security Aspects (Version 12.1.0 Release 12)*, 3GPP, Tech. Rep. TS 33.303, 2014.

[25] J. Urama *et al.*, "Dynamic social trust associations over D2D communications: An implementation perspective," in *Proc. IEEE Int. Conf. Mobile Services*, Jun. 2016, pp. 186–189.

[26] *Proximity-Based Services (ProSe); Stage 2*, 3GPP, Tech. France, Rep. TS 123.303 V12.2.0, 2014.

[27] C. Adams and S. Lloyd, *Understanding PKI: Concepts, Standards, and Deployment Considerations*. Reading, MA, USA: Addison-Wesley, 2003.

[28] A. Shamir, *Identity-Based Cryptosystems Signature Schemes*. Berlin, Germany: Springer, 1985.

[29] *Implementing Secure LTE-Assisted D2D Framework for Unreliable Cellular Connectivity*. (Oct. 2015). [Online]. Available: http://winter-group.net/d2d-security-lte-advanced-network/

[30] A. Ometov, A. Orsino, L. Militano, G. Araniti, D. Moltchanov, and S. Andreev, "A novel security-centric framework for D2D connectivity based on spatial and social proximity," *Comput. Netw.*, vol. 107, no. 2, pp. 327–338, Oct. 2016.

[31] A. Pyattaev, K. Johnsson, A. Surak, R. Florea, S. Andreev, and Y. Koucheryavy, "Network-assisted D2D communications: Implementing a technology prototype for cellular traffic offloading," in *Proc. Wireless Commun. Netw. Conf. (WCNC)*, 2014, pp. 3266–3271.

[32] A. K. Lenstra and E. R. Verheul, "Selecting cryptographic key sizes," *J. Cryptol.*, vol. 14, no. 4, pp. 255–293, 2001.

[33] H. Orman and P. Hoffman, "Determining strengths for public keys used for exchanging symmetric keys," *Internet Soc.*, vol. RFC 3766, pp. 1–23, Apr. 2004.

[34] H. Horsburgh, "The ethics of trust," *Phil. Quart.*, vol. 10, no. 41, pp. 343–354, 1960.

[35] M. Deutsch and M. Jones, "Cooperation and trust: Some theoretical notes," in *Proc. Nebraska Symp. Motivat.*, Oxford, England, 1962, pp. 275–320.
[36] W. Pearce, "Trust in interpersonal relationships," *Speech Monographs*, vol. 41, no. 3, pp. 236–244, 1974.
[37] J. D. Lewis and A. Weigert, "Trust as a social reality," *Social forces*, vol. 63, no. 4, pp. 967–985, 1985.
[38] C. L. Corritore, B. Kracher, and S. Wiedenbeck, "On-line trust: Concepts, evolving themes, a model," *Int. J. Human-Computer Stud.*, vol. 58, no. 6, pp. 737–758, 2003.
[39] S. Ruohomaa and L. Kutvonen, "Trust management survey," in *Trust Manage.*, 2005, pp. 77–92.
[40] S. Kiesler, J. Siegel, and T. W. McGuire, "Social psychological aspects of computer-mediated communication," *Amer. Psychologist*, vol. 39, no. 10, pp. 1123–1134, 1984.
[41] R. Rojas, *Neural Networks: A Systematic Introduction*. Springer Science & Business Media, 2013.
[42] J. Scott, *Social Network Analysis*. Thousand Oaks, CA, USA: SAGE, 2012.
[43] R. S. Burt, M. Kilduff, and S. Tasselli, "Social network analysis: Foundations and frontiers on advantage," *Annu. Rev. Psychol.*, vol. 64, pp. 527–547, 2013.
[44] R. S. Burt, "The network structure of social capital," *Res. Org. Behavior*, vol. 22, pp. 345–423, Jan. 2000.

ALEKSANDR OMETOV received the M.Sc. degree from the Department of Electronics and Communications Engineering, Tampere University of Technology (TUT), Finland, in 2016, and the Specialist degree in information security from the Saint Petersburg State University of Aerospace Instrumentation, Saint Petersburg, Russia, in 2013. He has been a Research Assistant with TUT since 2013. His major research interests are wireless communications, information security, heterogeneous networking, cooperative communications, and machine-to-machine applications.

EKATERINA OLSHANNIKOVA received the Specialist degree in history and theory of fine art from the Saint Petersburg State University of Technology and Design, Saint Petersburg, Russia, in 2013. She is currently a Project Researcher with the Department of Pervasive Computing, Tampere University of Technology, Finland. Her major research interests are in big social data, augmented and virtual reality, proximity- and location-based services, human-computer interaction, and user experience design.

PAVEL MASEK received the B.S. and M.S. degrees from the Department of Telecommunication, Brno University of Technology, Czech Republic, in 2011 and 2014, respectively, where he is currently pursuing the Ph.D. degree in teleinformatics. He has publications on a variety of networking-related topics in internationally recognized venues, as well as several technology products. His primary research interest lies in the area of wireless networks-M2M/H2H communication, cellular networks, heterogeneous networking, and data offloading techniques.

THOMAS OLSSON received the Dr.Tech. degree from the Tampere University of Technology (TUT), Finland, in 2012, with a thesis addressing user experience and user expectations of future mobile augmented reality systems. He is currently an Adjunct Professor and a Post-Doctoral Researcher with the Department of Pervasive Computing, TUT. He leads a Research Team, focusing on the user experience aspects of social proximity-based systems that aim to enhance social interaction between co-located people. He has co-authored over 60 research papers on user experience, augmented reality, ubiquitous computing systems, multidevice interaction, smart environments, haptic interfaces, and user expectations of new interactive technology.

JIRI HOSEK received the M.S. and Ph.D. degrees in electrical engineering from the Faculty of Electrical Engineering and Communication, Brno University of Technology (BUT), Czech Republic, in 2007 and 2011, respectively. He is currently a Senior Researcher with the Department of Telecommunications, BUT. His research work has been concentrated on the design of new communication mechanisms and services for mobile networks and measurement and prediction of end-user satisfaction with mobile data services (QoE).

SERGEY ANDREEV received the Specialist and Cand.Sc. degrees from the Saint Petersburg State University of Aerospace Instrumentation, Saint Petersburg, Russia, in 2006 and 2009, respectively, and the Ph.D. degree from the Tampere University of Technology in 2012. He is currently a Senior Research Scientist with the Department of Electronics and Communications Engineering, Tampere University of Technology, Finland. He has co-authored over 100 published research works on wireless communications, energy efficiency, heterogeneous networking, cooperative communications, and machine-to-machine applications.

YEVGENI KOUCHERYAVY received the Ph.D. degree from the Tampere University of Technology (TUT) in 2004. He is currently a Full Professor and the Lab Director with the Department of Electronics and Communications Engineering, TUT, Finland. He has authored numerous publications in the field of advanced wired and wireless networking and communications. His current research interests include various aspects in heterogeneous wireless communication networks and systems, the Internet of Things and its standardization, and nanocommunications. He is an Associate Technical Editor of the *IEEE Communications Magazine* and an Editor of the IEEE Communications Surveys and Tutorials.