Implementing Secure Network-Assisted D2D Framework in Live 3GPP LTE Deployment

Aleksandr Ometov†, Pavel Masek⋆, Jani Urama†, Jiri Hosek⋆, Sergey Andreev†, and Yevgeni Koucheryavy†
†Tampere University of Technology, Finland, Tampere, Korkeakoulunkatu 10, FIN-33720
⋆Brno University of Technology, Czech Republic, Brno, Technicka 3082/12

***Abstract*—Device-to-Device (D2D) communication constitutes an emerging network paradigm that promises to unlock decisive capacity gains without the need for expensive cellular resources. However, while deployment of this promising enabler technology in 5G-grade mobile networks is currently underway, the complete understanding of feasible use cases and their respective limitations has not yet been provided in literature. Today, employing D2D connectivity both in human-to-human and machine-to-machine scenarios, the attention of research community focuses on security, privacy, and trust. Inspired by this increasing demand, we provide in this paper a comprehensive summary on our live trial of secure cellular-assisted D2D communication technology within the full-featured 3GPP LTE network deployment. Correspondingly, we describe a novel D2D framework capable of delivering secure direct connectivity even if the managing cellular link is temporarily not available (unreliable), so that communicating devices could continue to exchange confidential data in their private coalitions. To this end, our prototype implementation characterizes the practical capabilities of secure D2D communication in dynamic, urban environments suffering from intermittent 3GPP LTE connectivity[1].**

I. Introduction and Motivation

The capability to utilize direct data exchange in modern wireless networks is currently facing the market with the popular WiFi-Direct technology [1], [2], which is already available in most of the contemporary mobile devices. Starting with their LTE Rel. 12 specifications, a novel set of enablers for proximity-based Device-to-Device (D2D) communication has also been offered by 3GPP [3]. The advantages of network-assisted D2D connectivity comparing to the traditional cellular links (i.e., direct connection vs. communication between eNodeB and user device) are many and include better spatial reuse as well as improved spectral and energy efficiency of the resulting communication system. However, a significant hurdle that slows the time-to-market of this promising technology is rooted in the fact that the users utilizing a direct connection may not have a reliable managing link to the cellular network. This limitation becomes critical as new important services begin to increasingly employ cellular networks. This includes, for instance, public safety and emergency systems for NSPS.

The previous research on cellular-assisted D2D conducted by our group [4], [5] confirms that by using the direct communication capability, cellular operators and mobile users receive a range of attractive benefits and opportunities. In particular, the Quality of Experience (QoE) and Quality of Service (QoS) levels may be improved dramatically. Inspired by these initial findings, we have recently implemented a live trial of assisted D2D technology basing on the experimental 3GPP LTE deployment located in Brno University of Technology, Czech Republic [6]. For the purposes of this trial, we utilized WiFi-Direct as a means for direct connectivity between user devices together with our proposed implementation of Proximity Services (ProSe) functionality [7], [8].

In the current work, continuing this line of research, we aim at enabling *secure* direct communication not only for the case of permanent (reliable) cellular connectivity, but also in situations when it becomes temporarily unreliable (unavailable). In other words, D2D users may "lose" their controlling cellular link, but can still continue exchanging confidential data as well as manage their secure coalition by adding and/or excluding some of the devices. This important use case raises many novel research questions related to the device's battery life, the computational requirements at the device side, as well as the real-time performance functionality of the entire communication chain, which significantly extends our previous results.

The rest of the paper is organized as follows. Section II is devoted to describing possible wireless technologies for D2D communication. Further, in Section III, 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 with the account of all the communication phases is provided in Section IV. Finally, the lessons learned during the implementation of the prototype as well as the key numerical results are summarized in the concluding Section V.

II. D2D Communication in Mobile Networks

The mobile networks of today are already facing a lack of bandwidth for its users and, hence, the list of candidate applications for proximity-based D2D communication is very long [9].

The most promising applications of D2D connectivity in next-generation cellular networks include offloading audio and video calls between proximate users, multimedia data sharing, gaming, as well as context-aware, public safety, and national security services [10]. More recently, *wearable communication* has emerged as the unprecedentedly large market. Wearable wireless devices (fitness bands, smart-watches, and augmented reality glasses) naturally exploit D2D channels for their efficient operation. Finally, direct communication is believed to become an important consideration not only to boost the information sharing and content distribution capabilities between the proximate human-controlled devices, but also enable a variety of use cases involving *machine-type communication* for home automation (smart measuring devices and sensors) [11] and vehicular communication (self-driven cars, traffic automation) [12], thus advancing the concept of the Internet of Things [13].

Today's market can supply us with a number of technology solutions that may be utilized for D2D system implementation. The most widely discussed candidates are IEEE 802.11 (WiFi) and IEEE 802.15.4 (BLE, ZigBee) technologies, all operating in unlicensed spectrum. Out of these, WiFi brings to developers more attractive opportunities in terms of delay, bandwidth, and coverage range. Augmenting WiFi-based communication capability between user devices, the WiFi-Direct technology [14] has been introduced relatively recently. It enables efficient direct connectivity without the need for infrastructure access points as well as provides a way to establish multiple overlapping networks at the same time.

In contrast to the above technologies, LTE-Direct specifications outline a communication system under the full control of a cellular network. However, as LTE-Direct technology is still under development, the resulting deployments are not expected by the mobile operators any time soon [15]. If implemented, the major concerns for running direct communication over the licensed bands would be cumbersome interface management, more complex transceiver design, and the need for additional standardization efforts. In case of WiFi-Direct, the built-in stock WiFi transceivers can be utilized and, therefore, our main focus remains on executing direct communication in the unlicensed bands. In light of the above, we have used the end devices equipped with WiFi transceivers in our corresponding trial of secure D2D communication.

III. Implementing Secure D2D Messaging

In order to **comprehensively trial our theoretical security-centric solution for D2D communication**, detailed in [16], we decided to construct a mobile application on top of Android platform. This application has the functionality of a secure messenger utilizing our proposed information security primitives. To familiarize the reader with the framework, we first outline the considered network architecture.

A. Test 3GPP LTE Deployment

The experimental 3GPP LTE deployment employed for the purposes of this prototype implementation is located in the laboratories of SIX Research Center at Brno University of Technology (BUT), Czech Republic. It is a practical, fully-operational cellular infrastructure with all the necessary system modules implemented in hardware. Our described LTE testbed (see Fig.1) serves the purposes of research and education for 3 years already and its essential components are listed in Table I.

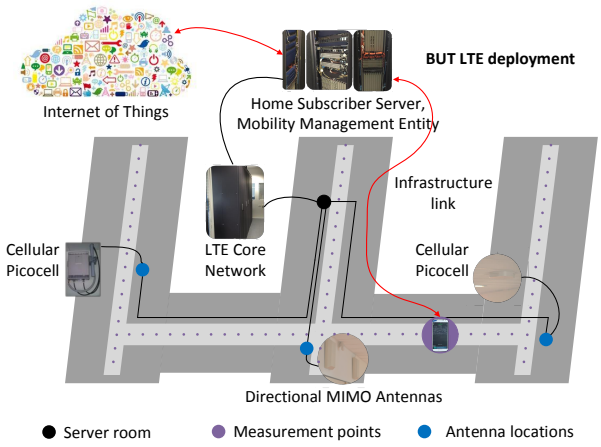

Fig. 1. Test 3GPP LTE deployment: structure and main modules

TABLE I
MAIN COMPONENTS OF THE 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.

The corresponding heterogeneous Radio Access Network (RAN) components feature three 700 MHz indoor cells operating in band 17 (AT&T) and one 1800 MHz cell where the key parameters are 5 MHz FDD with 2x2 MIMO. Further, EPS-IMS network includes the implementation of one outdoor cell in band 3 (1800 MHz). Together with the said LTE cells, three WiFi access points (APs) operating in 2.4 GHz and 5 GHz ISM bands are incorporated to offer the packet-switched data access services (e.g., VoIP, VoLTE) over LTE and WiFi RAN infrastructure. The Evolved Packet Core (EPC) enables high data rate services (up to 40 Mbps for download and up to 16 Mbps for upload) with the appropriate QoS and QoE provisions (up to 100,000 served user devices are supported). This full-featured deployment mostly accommodates our research and educational purposes by allowing full access to the experimental cellular network in order to obtain deeper understanding of its operation as well as open door to rapid and efficient prototyping of new technology.

B. Modifying D2D-Specific Modules

In order to enable our intended trial, several modifications to the experimental LTE system had to be done. First, we developed an additional server application that supports IPv4-based communication between mobile devices in addition to security certificate generation and distribution functionality. The main purpose of the latter is to allow for secure communication over LTE and WiFi radio interfaces.

A major benefit of direct connectivity is communication without the need for any infrastructure hot-spots. In other words, users can communicate directly even outside of network coverage, both WiFi and LTE. In this case, users would face a challenge of secure connection establishment, that is, when the managing entity is not directly available. Broadly, the modern wireless networks widely use the IPv4 protocol, and thus each of the mobile users in the network acquires a public IP address for its data connectivity. This address is conventionally provided by the cellular infrastructure.

In case of network-assisted D2D connectivity, IP addresses for users that communicate over a direct channel are also generated by the 3GPP LTE core when it has a reliable link to the corresponding server. For D2D communication outside of cellular coverage, new rules and routing protocols should be constructed. In connection to the above, the effective firewall policies applied inside the cellular network core may restrict direct access from one device to another and hence limit the direct communication opportunities. Therefore, we have implemented an additional firewall policy to allow for direct connectivity between the cellular network users and the network server. To this end, we utilized a specifically-defined port in order to offer the proof of the concept, see Fig. 2.

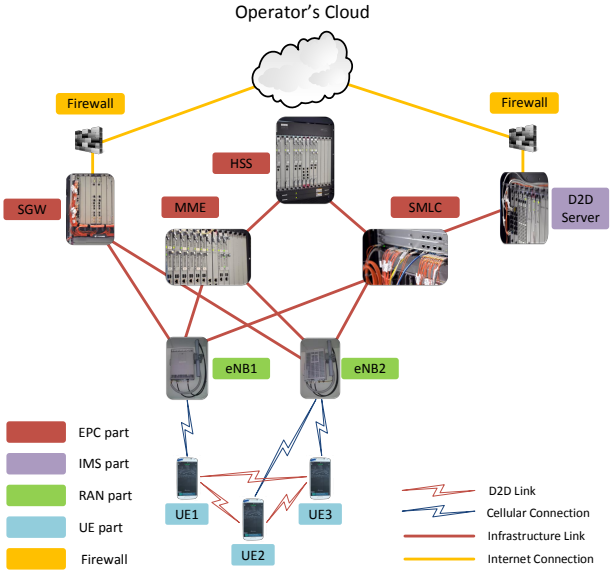

Fig. 2. Prototype implementation of a D2D system

C. Implementing Secure D2D Scenario

In a nutshell, our envisioned network-assisted D2D system is assumed to be controlled by the LTE infrastructure and builds upon the security protocols described in [17]. To this end, mobile users may establish and utilize a direct link only if they have a reliable connection to the ProSe server that is responsible for key and connection management.

Currently, secure communication is orchestrated by the Public Key Infrastructure (PKI) on top of the operator's network [18]. However, this solution can only be used in cases when the cellular link is available to all the devices under control. However, the mobile users do not have feasible means to continue their communication in case such cellular connection becomes unreliable (unavailable). This is due to the character of control coming from the cellular network as well as due to the centralized architecture of the LTE system. In order to keep the direct connection fully operational, D2D users have to employ distributed security solutions [19]. User devices out of cellular coverage would face such novel challenges as distributed discovery, authentication, trust and privacy maintenance, which are currently handled by the service residing in the operator's core.

Today, distributed mobile networks with some form of cellular assistance cannot be controlled by the LTE system if there is no reliable connection to the server. Further, network topology dynamics and unpredictable changes in trust relationships between the users should be tracked back and reported to the network as soon as any of the involved users reach cellular coverage. Therefore, solutions from the field of conventional ad hoc networks are not directly applicable in this context. In what follows, we briefly discuss the main operation modes of the proposed protocol in cases of both reliable and unreliable cellular connectivity.

In this work, we present a characteristic example of cellular-assisted, secure D2D network operation, where the reachable system states are shown in Table II. For the ease of implementation, it does not fully conform to the 3GPP operation model, but allows the direct connectivity also in the cases of intermittent cellular coverage. Importantly, device discovery phase is assumed to still be handled by the operator's ProSe functionality, and is not discussed in this work. Therefore, we assume that a cellular network serves as a Certificate Authority (CA) for all its mobile devices. Each of them has an unique ID and obtains a certificate signed by the CA whenever this device first associates with the cellular network. The user certificate is further utilized for the secure group establishment allowing to validate the involved users.

We begin with the secure group (coalition) *initialization* procedure, which is possible only under cellular network coverage, as it requires a reliable connection to the CA. Together with user certificates, the involved mobile devices receive their secrets and thus can initiate secure direct communication with each other. When one of the users is willing to establish a secure group with another, a corresponding request containing the IDs of the future group participants is issued to the corresponding server in the network. Then, the server triggers a polling procedure to ensure that the users desire to join the group. After the confirmation has been received, the CA generates a group certificate and a group secret based on

Lagrange polynomials, as it is detailed in [16]. After these initial steps, secure direct communication may continue over any conventional IP network.

We emphasize that secure communication within the group remains fully operational even in cases of unreliable cellular connectivity, as the users do not communicate via the server but transmit data directly. Moreover, based on key sharing schemes, the users in a secure group can take advantage of collaborative voting whenever they are willing to include a new user into the coalition or exclude an existing one from it. The users can perform group voting in two distinct cases: when all of them have a connection to the CA or, otherwise, when at least one of them does not have it.

In the case of reliable cellular connectivity, the procedure of joining or leaving the group is orchestrated by the server. Based on the votes of group members, it generates and distributes new group certificates for the modified coalition. On the other hand, if the server is unreachable for at least one of the devices, the users have to vote inside their coalition and such operation may be performed via *indirect* group secret reconstruction based on a preset threshold value. Finally, the users of the modified group can reconstruct a *secret share* to add a new device or regenerate their shares to exclude an undesirable user (e.g., the one violating group policies). Clearly, share regeneration and polling procedures consume additional computational power and require extra signaling as compared to the conventional infrastructure-based operation. On the other hand, our system offers improved QoS and connectivity experience for the network users. In the following section, we discuss our implemented scenario and concentrate on the proposed protocol details.

IV. Our Characteristic Secure D2D Scenario

In this section, our prototype implementation is detailed. We additionally discuss the proposed protocol operation that is also illustrated by the summary live-trial video in [20].

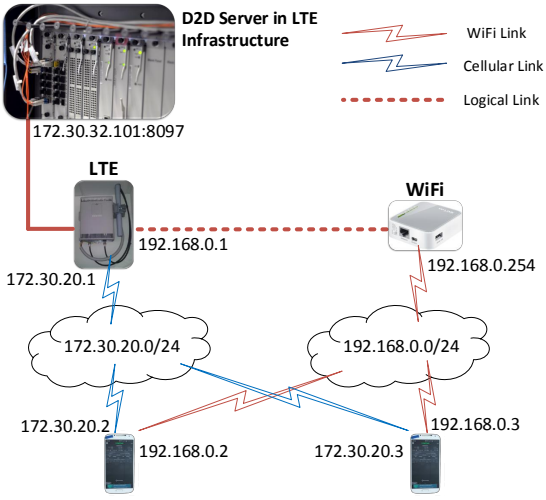

Fig. 3. Target scenario of secure D2D communication

TABLE II
D2D Network Operation Modes 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

For this demo implementation, we utilized the LTE system with a server running inside the core, see Fig. 3. The D2D server is represented as a Linux machine that has a Python service running in the background. The role of the latter is not only to act as the CA, but also manage authentication and logical IP association procedures. We used the Easy-RSA library as a component of the OpenVPN framework for certificate generation. In our demo, we also employed Android-based smart-phones, Samsung Galaxy S4, running non-rooted firmware version 4.4.2. (see Fig. 4). In the test mobile application, we implemented a modified Shamir Secret Sharing scheme focusing on the *java.security.** library. Due to the limitations of WiFi-Direct on Android, we decided to use an isolated WiFi AP running OpenWRT to emulate the distributed network. A characteristic scenario for our demo is described in what follows.

A. Target Application Setup

First, we begin by describing the group initialization stage. Three devices are connected to the cellular network and their users are starting the application, which generates public and secret keys for each user. The CA public key is already embedded into the application. Hence, each of the devices connects to the server inside the LTE core by using the TCP sockets and all the initial signaling is signed by the CA's public key. The user's public key is then sent to the server and associated with the user's unique ID – *Username@PublicIP*. Further, the server generates a certificate for each user and signs it with the *root* certificate. The server also sends user certificates and secrets to the corresponding owners, while the public keys are forwarded to other users upon request. By this, direct D2D communication on top of the cellular network becomes feasible.

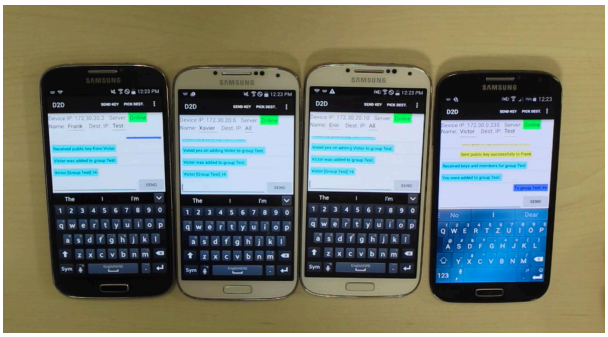

Fig. 4. Snapshot of our running demo, see [20] for details

B. Coalition Initialization

Our second proposed procedure relates to coalition creation (see Table II) and may be utilized in cases ③ and ④. The

server has complete knowledge on the users in proximity. Suppose that one out of three users is willing to build a secure coalition. The user device is then sending a request to the server regarding its proximate users and receives a list of their IDs over a cellular link. The initiating user can further choose which of these users will be invited into the future coalition. After selecting the invited users, the initiating device is sending this list to the server.

Further, polling is triggered by the server side, i.e., each of the users in the list is requested as to whether it would be willing to join the coalition. The responses from each device are also sent to the server. After the answers have been delivered or a timeout has been reached, the server is generating a group certificate for the coalition. In essence, the group secret is generated based on a Lagrange polynomial sequence, and a threshold value for adding and removing users from the group is set, whereas each user certificate is now being signed by the secure group certificate. In addition, user certificates are updated on the user side over a cellular link.

C. Voting in Existing Coalition

1) Reliable Connection to the Server: Our third possible scenario is adding a user in case of a reliable connection to the server, see Table II, and this procedure may occur in mode ④ as part of the voting process. Here, one of the devices included into the existing coalition is requesting the server to add a new device that is not yet a part of it. The respective request to the server contains the group name and the ID of the device to be added. A polling procedure is then triggered among the existing users regarding possible inclusion of this new user. Based on the preset voting threshold value, a decision is reached and the certificates are redistributed correspondingly as well as the coalition secret is updated. Exclusion of a user is performed in a similar manner. 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 Connection to the Server: In contrast, adding and removing users becomes a more complex task when the connectivity to the server becomes unreliable, i.e., in modes ① and ③. First, users should execute an instance of the routing protocol inside their distributed network, that is, user devices have to re-associate their IP addresses utilized when connected to the server. Regrettably, Android platform does not natively support such rerouting and hence we had to implement *our own routing solution*. Given that the unique device ID includes the IPv4 address together with the user name, where the former is used in the cellular network and cannot be changed manually from the device, the application can only interact with the IP on the WiFi interface. Assuming that the distributed network resides in a conventional LAN subnet of *192.168.0.0/24*, we eventually limit the maximum size of our secure coalition to 254 users. This is achieved by replacing one octet at the WiFi interface from the LTE interface, for instance, a device with the IP *172.30.20.**5*** on the LTE interface may suffer from unavailable connectivity to the server and thus the WiFi IP would be set to *192.168.0.**5***. By doing so, the users in the coalition are able to keep their connection running even without the centralized management.

By enabling direct connectivity between D2D devices even outside the cellular coverage, we had an opportunity to focus on the security protocol implementation in cases of unreliable cellular connectivity. Here, the devices should group together based on the concepts discussed in Section III-C. Continuing this line, we briefly describe the coalition joining procedure when the server is unavailable. Our additional requirement for supporting this case is for any new user to reside in 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 first send its public key (previously signed by the CA) to all the users in the coalition.

After an automated check of the credibility of the joining device, one of the existing users can invite this new user into the coalition by initiating the local polling. Then, the inviting device collects the responses and if the number of positive votes is above the threshold value preset in the coalition certificate, the procedure of the coalition secret reconstruction is initialized. In essence, it is a modified secret recovery scheme based on a Lagrange polynomial sequence, i.e., if k out of n devices group together, they can reconstruct the polynomial and obtain another *point* on the curve for the newly-joining user.

Finally, user exclusion without the reliable connectivity to the server is performed similarly. Here, the users group together and can change the Lagrange polynomial coefficients, that is, *scale* the curve, while at the same time keeping the coalition secret unchanged. At any moment of time, a device can leave the coalition by removing its certificate. Noteworthy, when the users are added to and excluded from the coalition, the *actual* participants store the chain of the respective modifications that is signed and distributed after each event. Based on this chain, the server can later receive a complete and trustworthy update on the events occurring to the coalition, while it has remained unreachable.

V. Conclusions and Lessons Learned

In this section, we discuss the important aspects that we faced during our prototype implementation, as well as offer the key numerical results and conclusions.

In the process of developing this demo, we solved a number of challenges regarding the LTE system operation, networking, and routing on the device side in addition to many smaller issues related to implementing security on Android. In particular, we had to (i) update the effective LTE firewall policies, (ii) develop and implement a custom routing protocol (LTE to WiFi), and (ii) construct a modified Shamir Secret Sharing scheme together with all the required modular algebra primitives tailored for Android.

Our main and the most essential learning while working with the real LTE core has been in that its DHCP server was not operating as expected. The devices were assigned IPv4

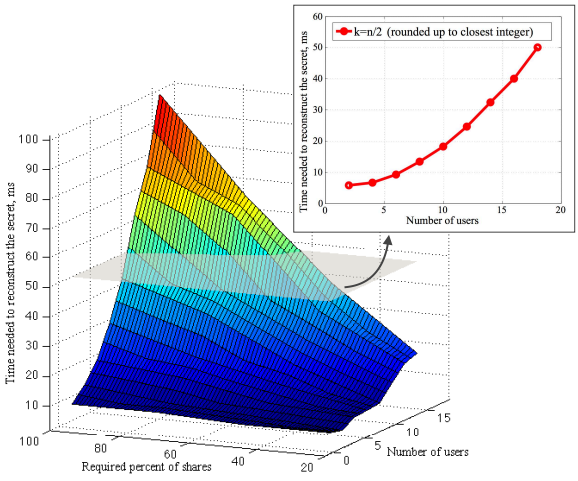

Fig. 5. Comparing the time to reconstruct a secret

addresses from the same pool, but from different, random subnets. Clearly, changing the subnetworks on the device side resulted in connectivity failures. To resolve these issues, we had to additionally conduct thorough traffic analysis to identify the said fault of the network configuration. In the end, LTE IP addresses and subnets have been set statically for each utilized SIM card. However, we are looking forward to having IPv6 support in next-generation networks, which we hope could resolve the routing and identification issues in a more comprehensive way.

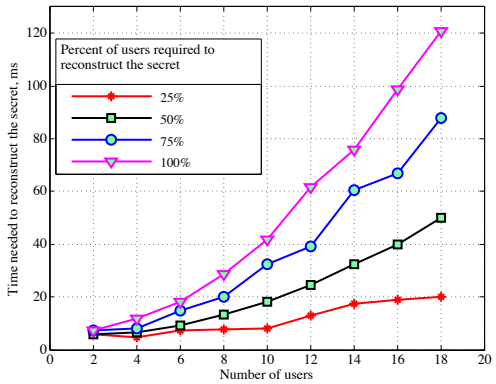

Fig. 6. Dependence of the recovery time on the threshold value of k

We have also tested our modified Shamir Secret Sharing scheme and calculated the time needed to reconstruct the secret on modern *non-restricted* smart-phones. The respective results are visualized in Fig. 5, where we observe that our proposed scheme is not taking more than 100ms to produce a new point for a newly-joining user or for excluding an existing user from the coalition. Further, Fig. 6 highlights the trade-off between the system operational complexity and the selected threshold value of k. Here, the level of trust is indicated in percents – the time of user inclusion/exclusion may vary dramatically as a result of the desired level of trust between the voting users.

In summary, the discussed numerical results may become an important consideration for resource-constrained devices (e.g., wearables), as the computational power of those may have difficulty to satisfy the requirements of the security primitives utilized by our current solution. Improving the proposed constructs with the methods of lightweight cryptography is therefore the ongoing direction of our research.

REFERENCES

[1] M. N. Tehrani, M. Uysal, and H. Yanikomeroglu, "Device-to-device communication in 5G cellular networks: challenges, solutions, and future directions," *IEEE Communications Magazine*, vol. 52, no. 5, pp. 86–92, 2014.

[2] L. Militano, M. Condoluci, G. Araniti, A. Molinaro, A. Iera, and F. H. Fitzek, "Wi-Fi cooperation or D2D-based multicast content distribution in LTE-A: A comparative analysis," in *Proc. of IEEE International Conference on Communications Workshops (ICC)*. IEEE, 2014, pp. 296–301.

[3] 3GPP TS 23.303, "TS 33.303 Proximity-Based Services (ProSe); Stage 2," Tech. Rep., 2014.

[4] A. Pyattaev, K. Johnsson, S. Andreev, and Y. Koucheryavy, "Proximity-based data offloading via network assisted device-to-device communications," in *Proc. of IEEE 77th Vehicular Technology Conference (VTC Spring)*. IEEE, 2013, pp. 1–5.

[5] A. Pyattaev, K. Johnsson, S. Andreev and Y. Koucheryavy, "3GPP LTE traffic offloading onto WiFi direct," in *Proc. of Wireless Communications and Networking Conference Workshops (WCNCW)*. IEEE, 2013, pp. 135–140.

[6] A. Pyattaev, J. Hosek, K. Johnsson, R. Krkos, M. Gerasimenko, P. Masek, A. Ometov, S. Andreev, J. Sedy, V. Novotny *et al.*, "3GPP LTE-Assisted Wi-Fi-Direct: Trial Implementation of Live D2D Technology," *ETRI Journal*, vol. 37, no. 5, pp. 877–887, 2015.

[7] A. Prasad, A. Kunz, G. Velev, K. Samdanis, and J. Song, "Energy-efficient D2D discovery for proximity services in 3GPP LTE-advanced networks: ProSe discovery mechanisms," *IEEE Vehicular Technology Magazine*, vol. 9, no. 4, pp. 40–50, 2014.

[8] 3GPP SP-110638, "LTE Proximity-Based Services Study Item," Tech. Rep., Sep. 2011.

[9] 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*. Springer, 2014, pp. 135–163.

[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, 2014.

[11] 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 und Informationstechnik*, vol. 131, no. 4-5, pp. 123–128, 2014.

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

[13] G. Wu, S. Talwar, K. Johnsson, N. Himayat, and K. D. Johnson, "M2M: From mobile to embedded internet," *IEEE Communications Magazine*, vol. 49, no. 4, pp. 36–43, 2011.

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

[15] LTE Direct, "The Case for Device-to-Device Proximate Discovery," Technical report, Qualcomm Research, Tech. Rep., 2013.

[16] 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. of IEEE 14th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom)*. IEEE, 2015.

[17] 3GPP, "TS 33.303 Universal Mobile Telecommunications System (UMTS); LTE; Proximity-based Services (ProSe); Security aspects (version 12.1.0 Release 12)," Tech. Rep., 2014.

[18] C. Adams and S. Lloyd, *Understanding PKI: Concepts, Standards, and Deployment Considerations*. Addison-Wesley Professional, 2003.

[19] A. Shamir, *Identity-Based Cryptosystems and Signature Schemes*. Springer, 1985.

[20] "Implementing Secure LTE-Assisted D2D Framework for Unreliable Cellular Connectivity," http://winter-group.net/d2d-security-lte-advanced-network/, October 2015.

View publication stats