Dynamic Social Trust Associations over D2D Communications: An Implementation Perspective

Jani Urama[†], Ekaterina Olshannikova[†], Aleksandr Ometov[†],
Pavel Masek[⋆], Sergey Andreev[†], Thomas Olsson[†], Jiri Hosek[⋆],
Jussi Niutanen[‡], Yevgeni Koucheryavy[†], and Tommi Mikkonen[†]
[†]**Tampere University of Technology**, Finland, Tampere, Korkeakoulunkatu 10, FIN-33720
[⋆]**Brno University of Technology**, Czech Republic, Brno, Technicka 3082/12
[‡]**Intel Finland**, Tampere, Insinöörinkatu 7, FIN-33720
Contact author's e-mail: *aleksandr.ometov@tut.fi*

***Abstract*—Network-assisted device-to-device (D2D) connectivity is a next-generation wireless technology that facilitates direct user contacts in physical proximity while taking advantage of the flexible and ubiquitous control coming from the cellular infrastructure. This novel type of user interactions creates challenges in constructing meaningful proximity-based applications and services that would enjoy high levels of user adoption. Accordingly, to enable such adoption a comprehensive understanding of user sociality and trust factors is required together with respective technology enablers for secure D2D communications, especially when cellular control is not available at all times. In this paper, we study an important aspect of secure communications over proximity-based direct links, with a primary emphasis on developing the corresponding proof-of-concept implementation. Our developed prototype offers rich functionality for dynamic management of security functions in proximate devices, whenever a new device joins the secure group of users or an existing one leaves it. To evaluate the behavior of our implemented application, we characterize its performance in terms of computation and transmission delays from the user perspective.**

I. Introduction and background

Today, the network data loads are growing tremendously. Based on the Visual Networking Index by Cisco, traffic transmitted over the wireless networks faced the increase of around 74% percent in 2015 [1]. Over the recent years, researchers have come to an expectation that the conventional networks are to be overloaded in less than a decade [2]. Therefore, the demand for novel connectivity enablers is also growing by leaps and bounds [3]. As one of the most prominent enablers, the research community anticipates network-assisted short-range communications to offer the much needed network capacity gains and at the same time facilitate the proliferation of proximity-based user applications and services. This emerging technology takes advantage of the cellular control layer while establishing a direct proximate connection between mobile users [4], [5], which brings various benefits such as the utilization of free-to-use unlicensed spectrum and higher data rates as well as the reductions in transmit power for the involved devices [6], [7]. Currently, industry is working intensively on the standardization of this promising technology [8], [9].

From the services point of view, the number of relevant scenarios is indeed high – from the use cases of National Security and Public Safety [10] to the proximity-based social interworking [11]. Presently, application developers and user-centric communities keep exploring and experimenting with the new forms of social interactions having the notion of "wireless sense" within the proximity-aware ecosystem [12]. We believe that the popularity of proximal, collective social applications is to keep growing over the following years and therefore in this paper we focus primarily on social user interactions. The main focus here is to harness local connectivity services facilitating communications between neighboring people and their personal devices located geographically close to each other. Apparently, the cellular networks of today are also suitable to accommodate the respective scenarios. However, cellular-assisted direct connectivity has to offer many advantages and may bring the additional benefits of lower latency, better battery efficiency, and higher user privacy.

The rest of this paper is organized as follows. In Section II, the motivation for the proof-of-concept (PoC) application development is given. Section III offers some numerical results to evaluate the usability of our implemented prototype. The last section concludes this work.

II. PoC implementation development

Our primary target in this research is to investigate hybrid centralized-distributed architectures as well as to enable secure data delivery for proximate D2D-based users under partial (weak) cellular connectivity. The below implementation extends our past theoretical work on securing network-assisted direct communications [13].

Whenever connected to the cellular network, a group of neighboring D2D users can straightforwardly establish their own secure associations. Should this connection become unavailable, our solution allows a set of user devices in the group to admit an additional (previously unassociated) device or to exclude one of the existing devices from the group. Presently, the considered group management relies on the cellular network employing the Public Key Infrastructure (PKI); our proposed algorithm develops such functionality

further and tailors it to the cases of partially unavailable cellular connection (in tunnels, airplanes, lifts, etc.). From the technology viewpoint, many contemporary mobile devices already have a number of available short-range radio interfaces (WiFi, BLE, etc.) as well as employ cellular connection (e.g., LTE) for most of their operation time. Hence, the proposed utilization of network-assisted WiFi-Direct radio assumes that the cellular network infrastructure controls D2D communications in all respects, including security, through the active cellular connection [14]. However, if this cellular link is becoming (temporarily) unavailable – secure communications may be disrupted and admission/exclusion of users to/from the secure communication groups would not be possible [15].

Fig. 1. Considered PoC prototype composition

In our envisioned scenario (given in Fig. 1), we consider all of the involved devices to be multi-radio terminals that initially have been connected to the infrastructure network, which has served as their trusted authority (TA) for the purposes of certificate distribution. Further, we assume that all of the devices participate in offloading cellular data traffic onto WiFi-Direct sessions; thus, we only account for the signaling information transfer over a cellular link [16]. This link is employed by D2D users in proximity to communicate with the PKI functions to establish a *coalition*, that is, a logical group of securely-communicating devices. Our proposed concept implies that whenever the managing infrastructure connection becomes unavailable for at least some of the devices in the coalition, additional measures are necessary to continue secure operation (communications, new user admission, user exclusion, etc.).

In the current implementation, we employ Android-based phones that run the 4.4 version of the operating system at the minimum. The server and the access point do not generally have any specific requirements, and we utilized Linux-based systems for the sake of development flexibility. These host the server application and provide IP connectivity in-between the server and the user devices. The client utilizes open-source Spongy Castle libraries [17], which are essentially the repackaging of the Bouncy Castle Java cryptography APIs [18] for Android that provides lightweight cryptographic solutions for Java-capable devices. The particular version used is 1.52.0. The server is running an application written in Python3, which provides the required functionality for the key generation, storage, and distribution. More specifically, the server application employs tools such as EasyRSA version 3.0 [19] and Python cryptography toolkit, PyCrypto version 2.6.1 [20], in order to generate RSA keys and X509 certificates.

The protocol operations available to our application can be broadly divided into three categories (see Fig. 2): *initialization*, *basic operations*, and *group operations*. The initialization phase allows generating a pair of temporary keys to secure the initial communications and authentication channel with the server [21]. Basic functions, such as sharing a public key and sending private messages to other group users with the known public keys, can be performed outside of any group. A certain client can also initiate a new group or it can be invited to join an existing group. All group members are capable of communicating messages within the group and may select other users that are to be added to or removed from the group. The latter actions (e.g., group member invites an outsider to join the group) trigger a majority vote procedure within the group. A client may also decide to leave the group at any time. Due to space constrains, we are not detailing the considered PoC operations in this work – please, refer to our previous paper for detailed information [22].

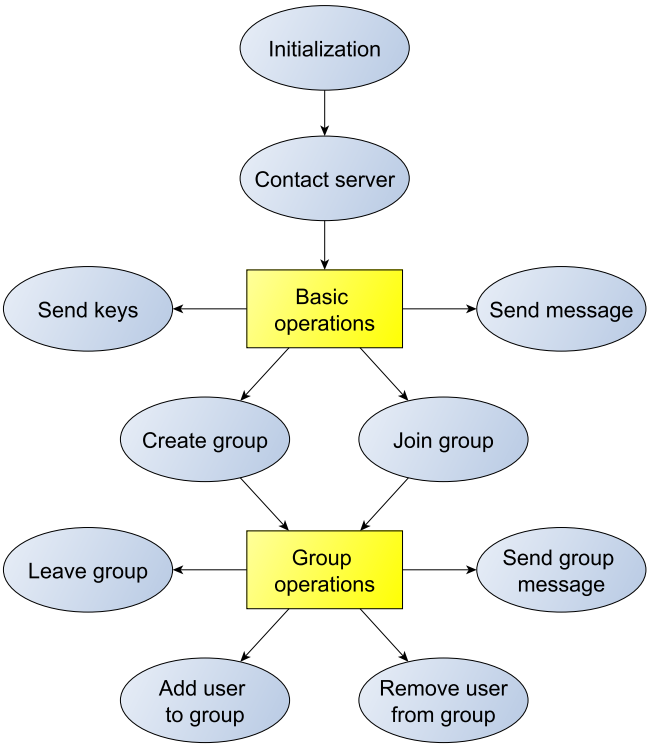


Fig. 2. Diagram of PoC application functionality

III. Usability Evaluation of our PoC Prototype

Further, we analyze the usability of our developed system. Recent research has shown that the key size required to

guarantee the acceptable level of security for modern devices is recommended to be not less than 1024 bits [23], [24], and is only expected to grow further for up to 3072 bits by 2030. Correspondingly, we evaluate how our considered protocol would be affected by such an increase from both computation and transmission points of view. As one of the most important service aspects faced by the users is the time they spend waiting before the actual communications would commence, we decided to evaluate the average delay for a key pair to be generated, distributed, and regenerated for both cases, i.e., when the user device has a reliable connection to the server and when it is outside of cellular coverage.

According to the proposed protocol, a user has to obtain an initial public and secret key pair in order to enable the secure communications between the devices. If the user has a connection to the server, said pair is generated automatically and sent to the device over a secure channel. On the other hand, if the user does not have a reliable cellular connection, the key pair is generated locally and user's public key may be disseminated to the proximate neighbors directly. To this end, Fig. 3 illustrates the corresponding execution times for the key generation cases in order to compare the computational capabilities of a modern phone and an average server. As we observe in the plot, user equipment is spending from 5 to 30 times more to generate a key pair for the current version of the protocol, i.e., when the key size is set to 1028 bits. In case of 4096 bits per key, the results vary from 30 up to 100 times. We can thus conclude that the key generation time of over a hundred seconds is unacceptable for everyday use, but our current approach executes in up to three seconds.

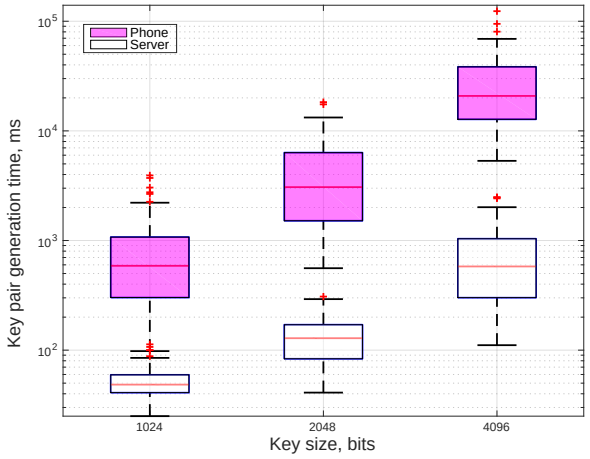


Fig. 3. Key pair generation time: server and user equipment

To further analyze our PoC prototype implementation, we test the operation of the network comprising four devices. As a case study, we assume a scenario where a user is automatically accepted or excluded during the voting procedure (i.e., a PPDR use case [10]). This is done to evaluate the device and the network performance without the impact of a human user. In Fig. 4, the key distribution from the server to the end-user device is presented for the 2048 bits key size. These results include the time needed to establish a connection (i.e., open a socket, etc.), transmit, and process data. To the best of our knowledge, such results are *transparent* for the user and may thus become a useful reference point for future implementations or improvements.

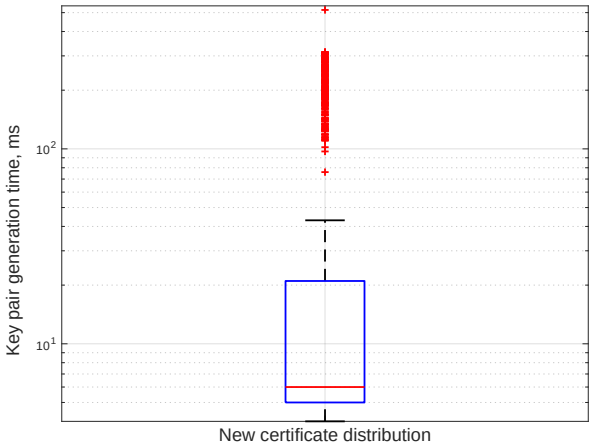
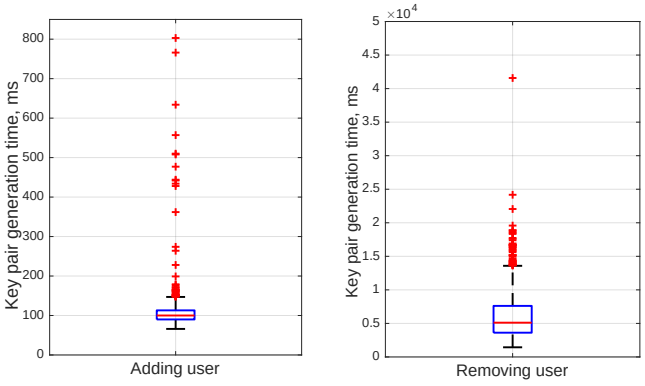


Fig. 4. Certificate delivery time

Finally, we study our protocol operation in the "ad hoc" (out-of-coverage) mode based on the previously-discussed case. The corresponding results are summarized in Fig. 5. In this scenario, generating a share for a new user takes approximately the same time as compared to distributing it by the server. However, the results may vary due to unpredictable behavior of the underlying random-access channel. Interestingly, even for such a small number of users the regeneration of coefficients and shares may significantly impact communications, while utilizing the key of a given size. Indeed, it may require up to 5 seconds to exclude a user from the secure group in the worst case.



(a) Add user procedure (b) Remove user procedure

Fig. 5. Operation time in the "ad hoc" mode

IV. Future work and conclusions

The developed secure D2D-based PoC application is only a first research step on social trust associations in proximity-based services. The goal of our further study is to provide

a vision on how the knowledge from multiple disciplines could be integrated to shift the social group formation to semantic level. We believe that it will bring an insight not only for our work on this topic, but also benefit the broad D2D-focused research 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 large number of contributions [25], [26], [27], [28]. 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 [29]. Therefore, there are many meanings and interpretations of trust and the ways to reach it. We plan to integrate the notion of trust into the D2D-based interworking as part of our further work on the topic.

In this work, we developed and evaluated a PoC application that allows for a group of neighboring devices that have their D2D communications controlled and maintained by the cellular network to establish dynamic connections. The implemented functionality has been summarized in this contribution and includes the capabilities of adding new users to a secure coalition as well as excluding the existing users from it even in the cases when a reliable cellular network connection turns out to be unavailable. Based on this PoC implementation, we performed a more detailed 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 for the first time report on the practical performance and limitations of secure network-assisted D2D connectivity for realistic system parameters.

ACKNOWLEDGMENT

Research reported in this paper was financed by the Academy of Finland, the National Sustainability Program under grant LO1401, and the Foundation for Assistance to Small Innovative Enterprises (FASIE) within the program "UMNIK" under grant 8268GU2015 (02.12.2015).

REFERENCES

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

[2] Ericsson AB, "Ericsson mobility report: On the pulse of the Networked Society," http://www.ericsson.com/mobility-report, February 2016.

[3] S.-P. Yeh, S. Talwar, G. Wu, N. Himayat, and K. Johnsson, "Capacity and coverage enhancement in heterogeneous networks," *IEEE Wireless Communications*, vol. 18, no. 3, pp. 32–38, 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*. Springer, 2014, pp. 135–163.

[5] 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.

[6] H. Luo, R. Ramjee, P. Sinha, L. E. Li, and S. Lu, "UCAN: a unified cellular and ad-hoc network architecture," in *Proc. of the 9th annual international conference on Mobile computing and networking*. ACM, 2003, pp. 353–367.

[7] L. Militano, A. Orsino, G. Araniti, A. Molinaro, and A. Iera, "A Constrained Coalition Formation Game for Multihop D2D Content Uploading," *IEEE Transactions on Wireless Communications*, vol. 15, no. 3, pp. 2012–2024, March 2016.

[8] K. Doppler, M. Rinne, P. Janis, C. Ribeiro, and K. Hugl, "Device-to-Device Communications; Functional Prospects for LTE-Advanced Networks," in *Proc. of IEEE International Conference on Communications Workshops (ICC)*, June 2009, pp. 1–6.

[9] G. Baldini, S. Karanasios, D. Allen, and F. Vergari, "Survey of wireless communication technologies for public safety," *IEEE Communications Surveys & Tutorials*, vol. 16, no. 2, pp. 619–641, 2014.

[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] E. Cho, S. A. Myers, and J. Leskovec, "Friendship and mobility: user movement in location-based social networks," in *Proc. of the 17th ACM SIGKDD international conference on Knowledge discovery and data mining*. ACM, 2011, pp. 1082–1090.

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

[13] 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)*, vol. 1. IEEE, 2015, pp. 826–833.

[14] A. Orsino, M. Gapeyenko, L. Militano, D. Moltchanov, S. Andreev, Y. Koucheryavy, and G. Araniti, "Assisted Handover Based on Device-to-Device Communications in 3GPP LTE Systems," in *IEEE Globecom Workshop on Emerging Technologies for 5G Wireless Cellular Networks*, 2015.

[15] G. Araniti, F. Calabro, A. Iera, A. Molinaro, and S. Pulitano, "Differentiated services QoS issues in next generation radio access network: a new management policy for expedited forwarding per-hop behaviour," in *Proc. of 60th Vehicular Technology Conference (VTC2004-Fall)*, vol. 4. IEEE, 2004, pp. 2693–2697.

[16] 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.

[17] R. Tyley, "Spongy Castle – repackage of Bouncy Castle for Android," https://rtyley.github.io/spongycastle/, 2016.

[18] Tau Ceti Co-operative Ltd, "Legion of the Bouncy Castle Java cryptography APIs," https://www.bouncycastle.org/java.html, 2013.

[19] Open-Source OpenVPN development community, "Easy-RSA – A Shell-based CA Utility," https://github.com/OpenVPN/easy-rsa, 2013.

[20] Dwayne Litzenberger, "PyCrypto - The Python Cryptography Toolkit," https://www.dlitz.net/software/pycrypto/, 2016.

[21] V. Petrov, S. Edelev, M. Komar, and Y. Koucheryavy, "Towards the era of wireless keys: How the IoT can change authentication paradigm," in *Proc. of World Forum on Internet of Things (WF-IoT)*. IEEE, 2014, pp. 51–56.

[22] 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," *Computer Networks*, 2016.

[23] A. K. Lenstra and E. R. Verheul, "Selecting cryptographic key sizes," *Journal of cryptology*, vol. 14, no. 4, pp. 255–293, 2001.

[24] H. Orman and P. Hoffman, "Determining Strengths For Public Keys Used For Exchanging Symmetric Keys," *The Internet Society*, April 2004.

[25] H. Horsburgh, "The ethics of trust," *The Philosophical Quarterly*, pp. 343–354, 1960.

[26] M. Deutsch and M. Jones, "Cooperation and trust: Some theoretical notes." in *Proc. of Nebraska Symposium on Motivation*, vol. XIII. Oxford, England: Univer. Nebraska Press, 1962, pp. 275–320.

[27] W. Pearce, "Trust in interpersonal relationships," *Speech Monographs*, vol. 41, no. 3, pp. 236–244, 1974.

[28] J. D. Lewis and A. Weigert, "Trust as a social reality," *Social forces*, vol. 63, no. 4, pp. 967–985, 1985.

[29] C. L. Corritore, B. Kracher, and S. Wiedenbeck, "On-line trust: concepts, evolving themes, a model," *International Journal of Human-Computer Studies*, vol. 58, no. 6, pp. 737–758, 2003.