Validating Information Security Framework for Offloading from LTE onto D2D Links

Antonino Orsino
ARTS Lab., DIIES Dept.
University Mediterranea of Reggio Calabria
Reggio Calabria, Italy
antonino.orsino@unirc.it

Aleksandr Ometov
Dept. of Electronics and Communications Engineering
Tampere University of Technology
Tampere, Finland
aleksandr.ometov@tut.fi

***Abstract*—D2D communications is one of the key technologies to enable aggressive spatial frequency reuse in future evolution of cellular systems. While the standardization efforts are far from their final stage there is clear understanding that security is one of the major concerns for proximity services. This is especially the case when one or more communicating stations in a logical cluster do not have an active connection to the serving base station. In this paper we propose a solution for secure throughput optimized communications in D2D-assisted cellular system. In order to provide additional throughput, a game-theoretic optimization approach is considered by taking into account social relationships and devices proximity. The proposed solution is *agnostic* to the chosen D2D communications technology (i.e., WiFi or LTE) and suitable for any possible cluster combination in full and partial cellular coverage. Performance evaluation of the proposed security framework show that social proximity information available at the D2D devices may substantially improves the system performance in term of throughput with respect to the standard security procedures. Finally, for sake of completeness, the effect of mobility for the reference scenario is evaluated.**

I. Introduction

The amount of traffic transmitted over wireless networks has been constantly increasing over the last decade almost doubling each and every year. Particularly, according to Cisco Visual Network Index more than 70% increase has been registered in 2014 [1]. By the year 2020 UMTS forum expects more than 130 EB/month while now this value is three times smaller [2]. This extraordinary growth is stimulated by successful introduction of fourth-generation mobile cellular system (4G) in more than 130 countries and associated improvements user devices including smartphones and tablets. It is also known that by 2020 around 90% of the world's population over 6 years old will have a mobile phone. In overall, 4G has qualitatively increased the access data rates competing with other types of wireless solutions including WiFi and finally fulfilling the old promise to provide a seamless Internet service accessibility on the move [3].

In spite of a significant step forward, many believe that even the current level of cellular networks will soon become insufficient to satisfy the constantly growing customer needs for more traffic at the air interface. Furthermore, this trend is likely to continue with the advent of smart unattended devices accessing the next-generation cellular systems [4], [5]. An emerging response to the above developments is the deployment of denser pico- and femto-cells with smaller coverage areas [6] or temporary networks infrastructure [7]. Hence, additional challenges arise along the lines of interference mitigation between such diverse smaller cells. In addition to the interference aspects, the cellular industry would need to handle higher rental fees together with the increased deployment and service costs [8]. Nevertheless, the trend for network densification is considered today as a mainstream solution to upgrade the degrees of spatial reuse and heterogeneity and, thus, meet the steadily growing traffic demand in the *fifth-generation* 5G systems [9], [10].

In today's wireless networks, a significant proportion of traffic is produced by the peer-to-peer (P2P) applications and services that feature users communicating in close proximity [11]. From this perspective, the reliance on direct device-to-device (D2D) transmissions in future 5G networks may be regarded as another form of densification – not with the infrastructure-based equipment, but rather with opportunistic user-based small *cells*. Existing short-range radio technologies (e.g., WiFi) may already be used to enable D2D services by taking advantage of the lower-to-the-ground links with no need for additional infrastructure deployment costs. Therefore, D2D communications may be preferred whenever possible to offload P2P traffic between the neighboring users and thus avoid the use of a more expensive cellular resource [12], [13].

In light of above, our main target in this research is to study the resulting hybrid centralized/distributed architectures where proximity connections are used to improve the communications quality utilizing the information security procedures on top. The underlying goal is to allow *secure* data delivery for already communicating D2D users even in the cases of *unreliable* cellular connection, which may become temporarily unavailable due to a variety of different factors, such as user mobility, obstacles, etc. When connected to the centralized infrastructure, a group of D2D users can straightforwardly establish their own information security rules with conventional methods. Whenever LTE connection becomes unavailable, our solution empowers a certain number of user devices in this group to admit a previously unassociated device or to exclude one of the existing members from the group. This results in the dramatical variance of main communications metrics like delay, relevant throughput and computational time/energy efficiency and, therefore, we are trying to evaluate some of those metrics in this paper.

This paper is structured as follows. In next section we provide a brief technological overview on possible D2D technologies. Section III provides our system model and proposed

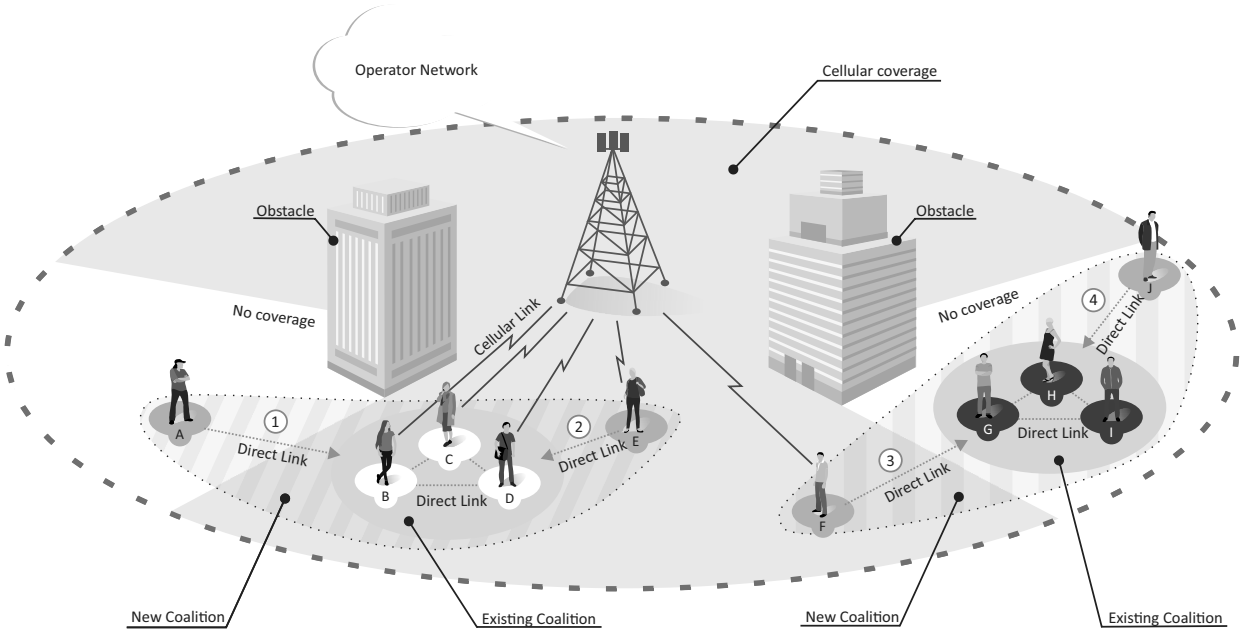

Fig. 1. Network-assisted D2D topology

game-theoretic approach. Further, in Section IV we evaluate applied approach to our information security frameworks and discuss obtained results.

II. Technological Overview

Recently, as part of the *Long Term Evolution* (LTE) cellular system development, various D2D connectivity mechanisms have been rapidly developing by the *Third Generation Partnership Project* as it is stated in 3GPP specifications: [14], [15], [16], [17]. As a consequence, the relevant standardization support is underway (coming in Release-12 and continued by Release-13) for a D2D technology operator to achieve efficient spatial reuse as well as provide proximal services and applications in future LTE deployments. Generally, D2D underlay operates on the same resources as the cellular network itself and a prominent candidate technology for the *licensed-band* D2D is often nicknamed as *LTE-Direct*. Essentially, the related concept has been proposed several years ago in [18] for the P2P partners in close proximity to exchange data over a direct link while sharing spectrum with the conventional cellular users. Simultaneously, the other branch of D2D communication development was establishing in *unlicensed-band*. Here, the attractive D2D benefits are available for utilization almost immediately, as the respective short-range *WiFi-Direct* technology is already implemented in most contemporary mobile devices [19], [20]. Precisely, unlicensed-band communications is historically subject to uncontrolled interference due to the lack of centralized power and channel access control. These can be made available to D2D partners with moderate degrees of cellular network assistance.

Summarizing all the above, today there is still no universal standard for the centralized control over the D2D communications [21]. In addition, another significant challenge at the stage of proximal discovery is the lack of suitable information security enablers [22]. However, we firmly believe that the remaining open research questions can all be solved promptly by further developing the network-assisted D2D solutions.

III. Enabling D2D Communications

A. System Model: Information Security Point of View

In this study we consider a base station providing coverage in a certain area. There is a number of mobile stations distributed over the landscape. We place no restrictions on their specific distribution and some of those might be out of the cellular coverage [23], as it is shown in Fig. 1. The nodes can be stationary or may move based on the chosen mobility model. To improve the spatial reuse of available resources, mobile nodes are expected to use direct communications whenever possible forming specific clusters depending on the type of applications in use and their proximity.

To increase the proposed framework efficiency, users are allowed to organize into the secure groups (clusters), based on two types of proximity metrics. First, there is *spatial proximity* of mobile users affecting the optimal clusters configuration with respect to the channel quality metric of interest. Optimizing this metric across all the mobile nodes we improve the data transmission performance of the system. The other type of the proximity is *social proximity* of users. A mobile device can be aware of previous contacts with other mobile users or, alternatively, this information can be obtained from the contacts stored on the device. Indeed, exploiting the social proximity of users to increase the performance of the proposed security algorithm we address the D2D cluster initialization phase improving the secure connection establishment time. Since the security algorithm is expected to work on top of the optimized clusterized network the initial clusterization of nodes ensuring optimized data transmission performance is done using game theoretic approach, a special subclass of classic optimization theory, by efficiently exploiting both

spatial and social proximity of mobile users, making this framework a base for the security algorithm.

Then, in order to provide a more comprehensive study about wireless network systems of today, the proposed framework takes into account the effect of users' mobility [24]. However, the classic optimization theory approach takes *snapshot* of a network at a certain instant of time t and aims to develop practical algorithms for optimized network performance with respect to a certain metric of interest. The reason to exploit game theoretic approaches in mobility environment is due to the complexity of keeping track of the past behavior of nodes due to the high dynamic nature of these networks. Generally, coalition games are applied in mobility scenarios to improve the cooperation among devices. In particular, a coalition is formed based on the cooperative devices and payoff allocation scheme is designed to guarantee an efficient cooperation within the coalition.

B. Utilizing Game-Theoretic Clusterization

In this section we introduce a typical coalition formation problem for cooperative D2D security procedures by clustering users in proximity and with social relationships. A traditional coalitional game is defined by $(\mathcal{N}, u)$ where $\mathcal{N} = \{p_1, \ldots, p_N\}$ is the set of N players and u is the utility function that models the value $u(T)$ for every set of players (coalition) $T \subseteq \mathcal{N}$. In addition, a coalitional game $(\mathcal{N}, u)$ is said to have *transferable utility* (TU) if the value of a coalition $u(T)$ can be arbitrarily divided between the coalition's players. If this is not true, then each player will have its own value in coalition T and the game is said with *non transferable utility* (NTU). In particular, for any coalition $T \subseteq \mathcal{N}$ the associated utility value $u(T)$ associated to a coalition T is equal to:

$$u(T) = \frac{\sum_{i=1}^{|T|} \sum_{j=1}^{|T|} s_{i,j} \cdot d_{i,j}}{|T|^2} \tag{1}$$

where $s_{i,j} \rightarrow [0, 1]$ is an asymmetric function (i.e., $s_{i,j} \neq s_{j,i}$) characterizing the social relationship or *friendship* between two devices defined in the $[0, 1]$ interval. In particular $s_{i,i}$ measures the willingness of a device in downloading the content exploiting a D2D connection with a friend in proximity instead than directly from the LTE infrastructure (i.e., eNodeB). The second term in equation (1) (i.e., $d_{i,j}$), indeed, is a binary function that yields 0 if the two devices are not in proximity, and 1 otherwise (in particular we set $d_{i,i} = 1$ by construction). Then, the result of the product of these two functions is averaged over all the considered elements for the given coalition T. It is worth noticing that the value of Eq. (1) will result in the $[0, 1]$ range. In particular, if the devices have the highest level of friendship and, at the same time, in mutual D2D coverage, the maximum value for a coalition $u(T) = 1$ is reached.

Considering, indeed, the utility definition we given in Eq. (1), and the notions of *transferable* and *non transferable* utility given at the beginning of this section, we can affirm that the studied game is an NTU game. The motivation is that the utility value of each player is personal, and, of course, is different for any player involved in the game; thus the utility value can not be evaluated globally and then divided among the players.

Further notions to introduce are the concept of *collection* of coalitions C defined as the set $C = \{C_1, \ldots, C_l\}$ of mutually disjoint coalitions $C_i \subset \mathcal{N}$ such that $C_i \cap C_{i'} = \emptyset$ for $i \neq i'$. If the collection contains all players in $\mathcal{N}$, i.e., $\bigcup_{i=1}^{l} C_i = \mathcal{N}$, then the collection is a *partition* Π or *coalition structure (CS)*. The set of all possible *coalition structures* is identified by $\Pi(N)$.

Given that finding the optimal solution is considered an NP-hard problem (i.e., the iterations should be performed among the all possible partitions in a given set of players), to characterize the feasible coalitional structure to form, we propose simple merge-and-split rules [25]. The key mechanism is to enable players to join or leave a coalition based on well-defined preferences so that each player is able to compare and order its potential coalitions based on which coalition it prefers to be a member of. To do this, let us introduce a preference relation over coalitions.

A *preference operator* $\triangleright$ is defined as $\mathcal{L} = \{\mathcal{L}_1, \ldots, \mathcal{L}_l\}$ and $\mathcal{Q} = \{\mathcal{Q}_1, \ldots, \mathcal{Q}_q\}$ for comparing two collections that are essentially partitions of the same subset $T \subseteq \mathcal{N}$, so that the same players are involved in the two collections. We say that $\mathcal{L} \triangleright \mathcal{Q}$, if the way $\mathcal{L}$ partitions T is preferred to the way $\mathcal{Q}$ partitions $\mathcal{S}$. The underlying criterion (i.e., the preference order) to be used for comparing two partitions can either be coalition payoff orders or individual payoff orders. In this paper, the preference order is defined according to the utilitarian order, that is, according to the *total value* of a coalition. Hence, we say that:

$$\mathcal{L} \triangleright \mathcal{Q} \Leftrightarrow \sum_{i=1}^{l} u(\mathcal{L}_i) > \sum_{j=1}^{q} u(\mathcal{Q}_j). \tag{2}$$

The so-defined preference order is at the basis of the two simple rules for the coalition formation game resolution.

Def. 1 (Merge Rule)**.** *Merge any collection of disjoint coalitions* $\{C_1, \ldots, C_k\}$ *if* $\{\bigcup_{i=1}^{k} C_i\} \triangleright \{C_1, \ldots, C_k\}$*, thus* $\{C_1, \ldots, C_k\} \rightarrow \{\bigcup_{i=1}^{k} C_i\}$.

Def. 2 (Split Rule)**.** *Split any coalition* $\{\bigcup_{i=1}^{k} C_i\}$ *if* $\{C_1, \ldots, C_k\} \triangleright \{\bigcup_{i=1}^{k} C_i\}$*, thus* $\{\bigcup_{i=1}^{k} C_i\} \rightarrow \{C_1, \ldots, C_k\}$.

The merge rule implies that two or more coalitions join to form a larger coalition if operating all together the utility obtained is greater than the utility obtained if the coalitions operate in a separate way. As a result, all players are able to improve the total utility. The split rule implies that a coalition splits into smaller coalitions if and only if the division does not introduce any negative effect on the total utility value. A split happens irrespective of the other players' preferences outside of that coalition. The objective of the players is to find a federation with maximum utility that is obtained through an iterative application of the merge and the split rules. It has been proved [25], that any iteration of successive arbitrary

merge and split operations *terminates*.

Once the merge and split operations are defined, the coalition formation game for the cooperative devices can be modeled. Starting from an initial partition $\Pi^{ini}(N) = \mathcal{N} = \{p_1, p_2, \ldots, p_N\}$, the merge and split rules are continuously iterated by the eNodeB until a convergence is reached. Therefore, the algorithm terminates when no merging or splitting occurred in the last iteration. In this case, the final resulting partition $\Pi^{fin}(N)$ will be adopted by the edge node (i.e, the eNodeB).

C. Securing Cluster Intercommunications

In modern cellular networks, the central control infrastructure orchestrating the associated wireless devices is assumed to be always available. Consequently, cellular network is typically assumed to serve as a *trusted authority* for security purposes. In proximity-based D2D communication with continuous cellular connectivity, the 3GPP LTE base station is responsible for managing security functions within the network, and most of the corresponding operations can be handled over the Public Key Infrastructure (PKI) [26]. On the other hand, for wireless architectures not relying on pre-existing infrastructure, communication and security functions are distributed across users [27], [28].

Although the D2D-assisted cellular system operation may, at the glance, look similar to ad hoc ones there is one key difference allowing to relax numerous restrictive assumptions of pure ad hoc systems. In a D2D case all the communicating devices are associated with the cellular base station at least for some time, facilitating distribution of initial security-related information (master keys, certificates, etc.). Hence, classical decentralized security-centric solutions (for e.g., sensor networks) may be significantly augmented in the D2D case by utilizing the possibility to (periodically) access the trusted cellular infrastructure.

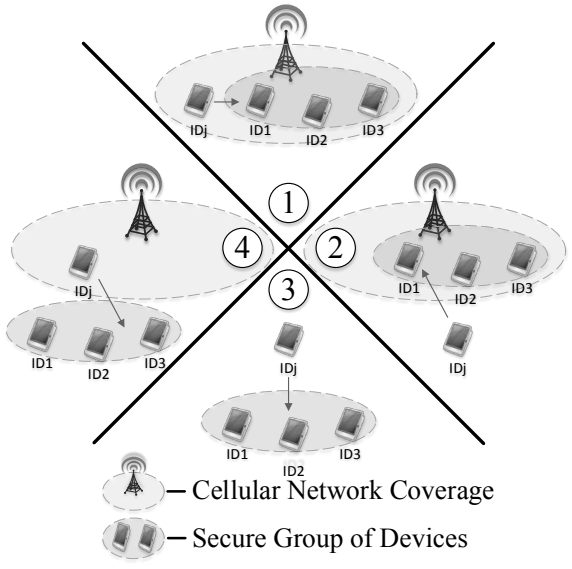

Fig. 2. Possible D2D operation cases: Information Security

When designing the security solution, we realized that the cellular network coverage is imperfect and sometimes users can face situations with unreliable cellular connectivity due to natural obstacles, tunnels, planes or other issues. However, while using proximity services like games, file sharing and data exchange, users are assumed to have a continuous support for those applications over secure channel. In order to understand what kind of functionality is needed for the security algorithm, we consider those connectivity cases sketched in Fig. 2. All the possible scenarios that may appear in D2D assisted network operation can be reduced to the four cases discussed below. Mode detailed description of the cases could be found in our recent work [22].

In the figure, we first focus on the group of devices in case ① that have already established their own coalition by employing a cellular connection to the operator network, the application server, and the PKI. The respective coalition secret has already been generated at the server side, and the users have received their corresponding credentials and certificates of each other. However, devices remain connected to the cellular network that orchestrates their direct communication. Here, j^{th} user is willing to join the coalition while having a connection to the cellular network. The application server processes the user request and, if the existing coalition accepts it, new certificates and public keys are delivered over the cellular link, while the coalition secret is updated accordingly.

Continuing with case ② a new user with no current cellular connection is willing to join the group by sending a request over a D2D link. The system should operate in a way similar to that for ad hoc networks. That is, the acceptance decision for the requesting device is made collectively – when k out of N devices in the coalition allow access for the new user, it joins. Importantly, the coalition secret would not be updated on the server side, and addition of this new user would be transparent for the overall network. Such operation is essential, as when the infrastructure link is restored for user, the operator network's PKI would remain in full control of the updated information security associations.

Finally, cases ③ and ④, i.e., the coalition does not have active cellular connection, can be regarded as a more complex scenario. In particular, in case ③ a new user is joining while having an infrastructure link, whereas the other users do not have active cellular connection. Here, all the key generation and distribution logic is carried out over the D2D links, as in case ②. In addition, these functions require a higher degree of user involvement e.g., into the key generation process, as well as into the voting procedures. To this end, the coalition secret is kept unchanged until when the considered group of devices restores their cellular network coverage.

IV. Evaluating Optimized Clustering

In this section we evaluate the performance of the proposed framework. Basically, recalling the structure of the proposed framework as a combination of the game theoretic clusterization and security algorithm we use a large-scale system level simulator to analyze performance of the proposed framework as a whole.

A. Security Algorithm

One of main framework issues is performance of the coalition joining procedure. Here we consider the two technologies for communications inside the cluster (i.e., WiFi-Direct and

LTE-Direct), the corresponding delays of joining the coalition are given by:

$$T_{LTE} = L_{U\to BS} + nL_{BS\to U} + nL_{U\to BS} + L(t^{f(x)}) + \\ + (n+1)L_{U\to BS}, \quad (3)$$

$$T_{WiFi} = 3W_{U_j} + 2nW_{U_i} + W(t^p) + k(W_{U_i} + t^s + t^r) + \\ + t^r + k(W_{U_i} + t^{-r}) + t^{-r}. \quad (4)$$

where n is a number of devices in a coalition, $L_{U\to BS}$ is the message transmitting time from cellular user to the cellular BS, $L_{BS\to U}$ is the time needed for the acknowledgement from BS, and $L(t^{f(x)})$ is the time for the polynomial sequence, certificates and keys generation. As for the second equation, here k is a threshold value of users needed to include/exclude a user in a cluster, W_{U_j} is the time needed to communicate between a coalition and a new user, W_{U_i} is communicating time between two users within the coalition, $W(t^p)$ is the time to generate all the protocol steps, t^s is the time experienced by the user to generate a share, t^r and t^{-r} are amount of time to add and remove salts.

In order to evaluate the information security framework operations, we performed a set of tests by considering a real-life environment. In particular, we exploited a "3GPP LTE-Assisted Wi-Fi-Direct" trial (i.e., available in [29]) implemented at Brno University of Technology, Czech Republic, in order to evaluate different RSA operation modes. As we can notice, the final conclusion is that performing security primitives by exploiting the powerful processor of the eNodeB results in a ten times less execution time with respect to the user side.

Further results have been obtained by considering the security framework execution time either with WiFi-Direct or LTE-Direct. As we can observe, using WiFi-Direct translates in worst execution time due to the high internal processing that the users have to perform to execute all the security procedures. However, the advantage in this case is that using *unlicensed bands*, users experienced a connectivity even if there is a lack of the network infrastructure.

B. Simulation results

To evaluate the performance of the information security approach, a simulation campaign has been performed by using the WINTERsim. The reference scenario consists of the LTE eNodeB cell with a round shape and a radius is equal to 100m [30]. Here, 100 UEs are uniformly distributed within the coverage area. We exploited the *Levy Flight* mobility model in order to characterize the patterns of the users moving pattern in a speed range $[0.2, 2.0]$m/s. Then, we modeled the multimedia traffic by considering a video streaming application with an inter-arrival time equal to 100ms and a packet size of 100Kb [31]. Here, WiFi link has the throughput of 40 Mbps and LTE link has 10 Mbps. Time to initialize D2D link is set to 1 second.

To provide a better understanding of the security framework effect on wireless systems, we focus on two system

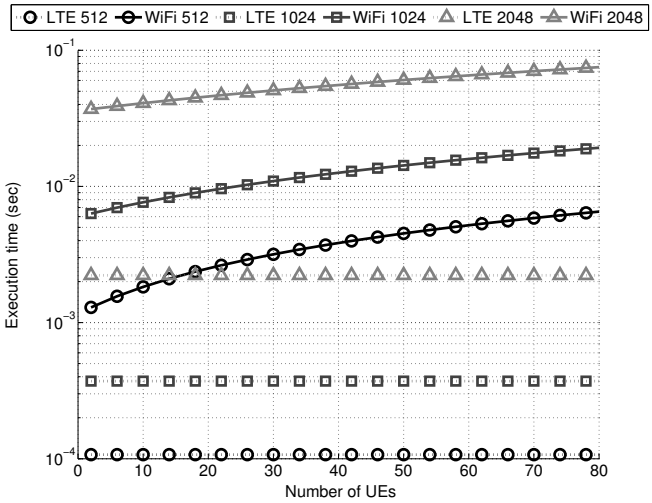

Fig. 3. Execution time for a join user procedure ($k = N/2$)

parameters given by (i) *UE latency* and (ii) *average UE relevant throughput*. In particular, the UE relevant throughput represents that amount of bits received by the users when they download the desired content either with a LTE or WiFi -Direct link. Then, we consider as a baseline algorithm for our study the security approach proposed [22].

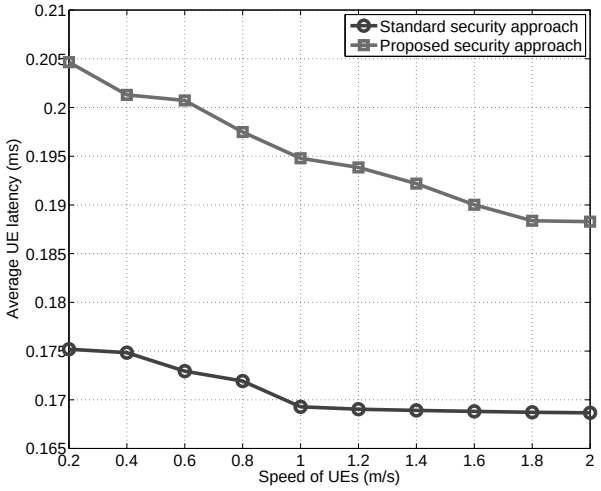

Fig. 4. Average UE Latency by varying the mobility intensity

The average latency is evaluated by varying the speed of users and the results are shown in Fig. IV-B. As we can notice, the latency decreases linearly with the mobility intensity. Increasing of the mobility intensity, indeed, translates in an higher number of contacts among the users. As a consequence, the users are more willing to download the multimedia content through WiFi-Direct with respect to LTE. Nevertheless, a security approach performed on a eNodeB-side overcomes the proposed solution. The motivation is that our security scheme introduces an additional delay when users are in proximity but

not under the network coverage. Nevertheless, the advantage of using new solution instead of the standard one is the fact that no connectivity could be provided when there is a lack of the network infrastructure.

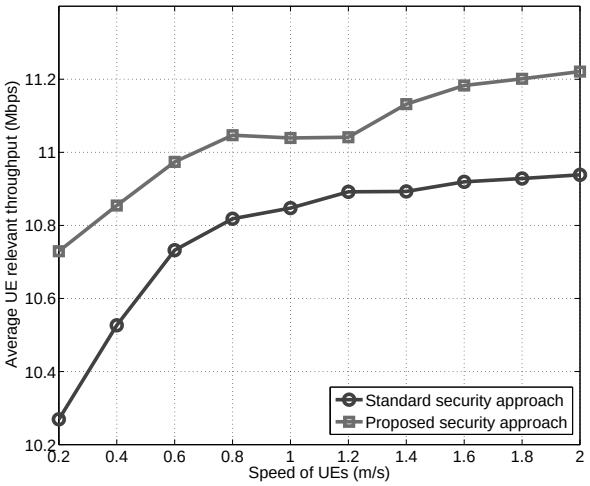

Fig. 5. Latency and throughput varying the speed of UEs (Number of users is set to 100)

The relevant throughput experienced by the users is shown in Fig. IV-B. As we can observe, the proposed security algorithm overcomes performance compared to the standard solution. This is due to the fact that our approach provides connectivity to users that are in a D2D transmission range but not in a LTE coverage. In such a case, the *additional* throughput is obtained at a cost of additional delay given by the establishment of a direct D2D connection in order to execute all the security procedures.

V. Conclusions

In this paper we evaluated a security framework for D2D communications in LTE systens. The proposed security approach is increasing the security signaling messages, but, at the same time, provides connectivity to users that are not in LTE network coverage. In order to shown the benefits of our novel scheme, a simulation campaign has been performed by considering typical system metrics such as UE latency and throughput. Obtained results show that exploiting D2D connections leads to an increased throughput for the users at cost of an additional delay (and energy consumption) given by the signaling messages exchanged locally in the cluster.

VI. Acknowledgments

The described research was supported by the Academy of Finland 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 update, 2014-2019," *White Paper*, February 2015.

[2] A. Ericsson, "Ericsson mobility report: On the pulse of the Networked Society," July 2015.

[3] S. Andreev, P. Gonchukov, N. Himayat, Y. Koucheryavy, and A. Turlikov, "Energy efficient communications for future broadband cellular networks," *Computer Communications*, vol. 35, no. 14, pp. 1662–1671, 2012.

[4] P. Masek, J. Hosek, and M. Dubrava, "Influence of m2m communication on lte networks," in *Sbornik prispevku studentske konference Zvule*, vol. 1, p. 2014, 2014.

[5] V. Petrov, S. Andreev, A. Turlikov, and Y. Koucheryavy, "On IEEE 802.16 m Overload Control for Smart Grid Deployments," in *Internet of Things, Smart Spaces, and Next Generation Networking*, pp. 86–94, Springer, 2012.

[6] M. Condoluci, M. Dohler, G. Araniti, A. Molinaro, and K. Zheng, "Toward 5G densenets: architectural advances for effective machine-type communications over femtocells," *IEEE Communications Magazine*, vol. 53, no. 1, pp. 134–141, 2015.

[7] G. Araniti, M. Sanctis, S. C. Spinella, M. Monti, E. Cianca, A. Molinaro, A. Iera, and M. Ruggieri, *Personal Satellite Services: Second International ICST Confernce, PSATS 2010, Rome, Italy, February 2010 Revised Selected Papers*, ch. Hybrid System HAP-WiFi for Incident Area Network, pp. 436–450. Berlin, Heidelberg: Springer Berlin Heidelberg, 2010.

[8] P. Marsch, B. Raaf, A. Szufarska, P. Mogensen, H. Guan, M. Farber, S. Redana, K. Pedersen, and T. Kolding, "Future mobile communication networks: challenges in the design and operation," *IEEE Vehicular Technology Magazine*, vol. 7, no. 1, pp. 16–23, 2012.

[9] S. Andreev, M. Gerasimenko, O. Galinina, Y. Koucheryavy, N. Himayat, S.-P. Yeh, and S. Talwar, "Intelligent access network selection in converged multi-radio heterogeneous networks," *IEEE Wireless Communications*, vol. 21, no. 6, pp. 86–96, 2014.

[10] O. Galinina, S. Andreev, M. Gerasimenko, Y. Koucheryavy, N. Himayat, S.-P. Yeh, and S. Talwar, "Capturing spatial randomness of heterogeneous cellular/WLAN deployments with dynamic traffic," *IEEE Journal on Selected Areas in Communications*, vol. 32, no. 6, pp. 1083–1099, 2014.

[11] 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.

[12] L. Militano, M. Condoluci, G. Araniti, A. Molinaro, A. Iera, and G.-M. Muntean, "Single Frequency-Based Device-to-Device-Enhanced Video Delivery for Evolved Multimedia Broadcast and Multicast Services," *IEEE Transactions on Broadcasting*, vol. 61, pp. 263–278, June 2015.

[13] L. Militano, A. Orsino, G. Araniti, A. Molinaro, and A. Iera, "A constrained coalition formation game for multihop d2d content uploading," *Wireless Communications, IEEE Transactions on*, vol. PP, no. 99, pp. 1–1, 2015.

[14] 3GPP TR 22.803, "Feasibility Study for Proximity Services (ProSe)." Release 12, June 2013.

[15] 3GPP TS 23.303, "Proximity Based Services (Stage 2)." Release 13, Dec. 2015.

[16] 3GPP TS 36.300, "Evolved Universal Terrestrial Radio Access (E-UTRA) and Evolved Universal Terrestrial Radio Access Network (E-UTRAN)." Release 11, Sept. 2012.

[17] 3GPP TS 36.213, "Evolved Universal Terrestrial Radio Access (E-UTRA): Physical layer procedures." Release 11, Dec. 2012.

[18] K. Doppler, J. Manssour, A. Osseiran, and M. Xiao, "Innovative concepts in peer-to-peer and network coding," *Celtic Telecommunication Solutions*, vol. 16, p. 09, 2008.

[19] 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. of Wireless Communications and Networking Conference (WCNC)*, pp. 3266–3271, IEEE, 2014.

[20] P. Masek, K. Zeman, J. Hosek, Z. Tinka, N. Makhlouf, A. Muthanna, N. Herencsar, and V. Novotny, "User performance gains by data offloading of LTE mobile traffic onto unlicensed IEEE 802.11 links," in *38th International Conference on Telecommunications and Signal Processing (TSP)*, pp. 117–121, IEEE, 2015.

[21] M. Condoluci, L. Militano, A. Orsino, J. Alonso-Zarate, and G. Araniti, "LTE-direct vs. WiFi-direct for machine-type communications over LTE-A systems," in *Proc. of IEEE 26th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC)*, pp. 2298–2302, IEEE, 2015.

[22] 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.

[23] D. Moltchanov, "Distance distributions in random networks," *Ad Hoc Networks*, vol. 10, no. 6, pp. 1146–1166, 2012.

[24] Y. Koucheryavy, D. Moltchanov, and H. Jarmo, "Impact of mobility on entertainment services' performance in heterogeneous wireless environment," *Proc. of Australasian Telecommunication Networks and Applications Conference*, 2003.

[25] K. R. Apt and A. Witzel, "A generic approach to coalition formation," *International Game Theory Review*, vol. 11, no. 03, pp. 347–367, 2009.

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

[27] Z. J. Haas, J. Deng, B. Liang, P. Papadimitratos, and S. Sajama, "Wireless ad hoc networks," *Encyclopedia of Telecommunications*, 2002.

[28] 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 IEEE World Forum on Internet of Things (WF-IoT)*, pp. 51–56, IEEE, 2014.

[29] 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.

[30] D. Moltchanov, Y. Koucheryavy, and J. Harju, "Loss performance model for wireless channels with autocorrelated arrivals and losses," *Computer Communications*, vol. 29, no. 13, pp. 2646–2660, 2006.

[31] D. Moltchanov, Y. Koucheryavy, and J. Harju, "Cross-layer modeling of wireless channels for data-link and IP layer performance evaluation," *Computer Communications*, vol. 29, no. 7, pp. 827–841, 2006.