A Novel Security-Centric Framework for D2D Connectivity Based on Spatial and Social Proximity

Aleksandr Ometov[a,c,*], Antonino Orsino[b], Leonardo Militano[b], Giuseppe Araniti[b], Dmitri Moltchanov[a], Sergey Andreev[a]

[a] *Tampere Univesity of Technology, Tampere, Finland*
[b] *University Mediterranea of Reggio Calabria, Italy*
[c] *Saint Petersburg National Research University of Information Technologies, Mechanics and Optics (ITMO University), St.Petersburg, Russia*

Abstract

Device-to-device (D2D) communication is one of the most promising innovations in the next-generation wireless ecosystem, which improves the degrees of spatial reuse and creates novel social opportunities for users in proximity. As standardization behind network-assisted D2D technology takes shape, it becomes clear that security of direct connectivity is one of the key concerns on the way to its ultimate user adoption. This is especially true when a personal user cluster (that is, a smartphone and associated wearable devices) does not have a reliable connection to the cellular infrastructure. In this paper, we propose a novel framework that embraces security of geographically proximate user clusters. More specifically, we employ game-theoretic mechanisms for appropriate user clustering taking into account both spatial and social notions of proximity. Further, our information security procedures implemented on top of this clustering scheme enable continuous support for secure direct communication even in case of unreliable/unavailable cellular connectivity. Explicitly incorporating the effects of user mobility, we numerically evaluate the proposed framework by confirming that it has the potential to substantially improve the resulting system-wide performance.

1. Introduction and motivation

The numbers of devices connected to contemporary cellular networks have been increasing dramatically over the last decade [1]. Tothis end, the traffic load has also been growing tremendously, where the mobile data per smartphone and tablet is expected to reach 5 GB and 17 GB per month, respectively [2]. In addition to conventional human-generated data, a plethora of the Internet of

*Corresponding author at: Department of Electronics and Communications Engineering, Tampere University of Technology, Tampere, Finland, FI-33720. Tel.: +358 44 9714624
Email address: aleksandr.ometov@tut.fi (Aleksandr Ometov)

Things (IoT) devices connect to the network as well [3]. This trend is likely to continue with the advent of smart wearable devices, all of which become part of the next-generation (5G) wireless ecosystem.

Market predictions behind wearables are such that these technologies are expected to soon bring completely new commercial opportunities. Recognizing this, Apple, Google, and Samsung are already on the technological edge in this field. However, small business is also expected to take its part in the race for the future of wearable computing. Meanwhile, the cellular systems of today are primarily focusing on their throughput optimization, which does not seem to be the main concern for such devices as smart watches and fitness trackers for which the quality of service (QoS) would require much further improvement over the following years [4].

Currently, communication technologies employed by most contemporary wearable devices are predominantly short-range. Vendors prefer utilizing BLE (Bluetooth low energy), WiFi or even NFC (Near Field Communication) radios to enable wearables reach their user's smartphone acting as the data aggregator, as it is demonstrated in Fig. 1. As it is expected that every second person with a smartphone would have at least one supplementary wearable device by 2020, the resulting network loads might increase significantly and lead to the degradation of QoS. Ultimately, distributed and uncoordinated wearable networks may just do to today's wireless technology what massive machine-type communication scenarios have already done to the cellular networks [5]. This aspect requires a careful research consideration.

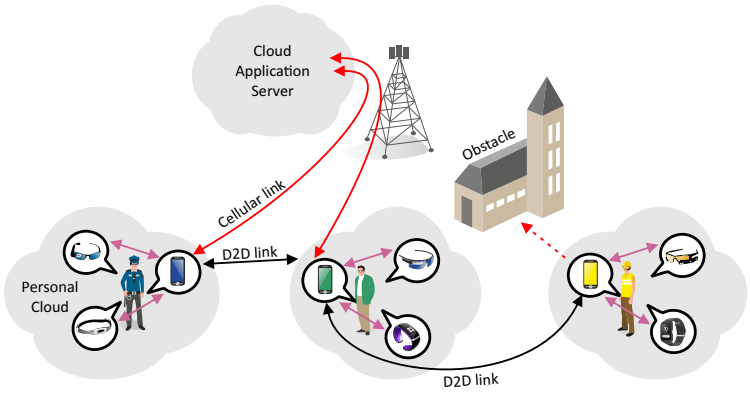


Figure 1: Urban wearable communications scenario.

In the near future, an increasing share of mobile traffic is expected to be produced by wearable applications and services that feature users in close proximity. In light of this, the reliance on direct device-to-device (D2D) transmissions in forthcoming 5G networks may be regarded as a vital technology to relieve the infrastructure-based cellular systems from this additional load. Existing short-range radio technologies may already be used to enable D2D connectivity by taking advantage of more efficient links without the need for additional infras-

tructure deployment costs. Therefore, D2D communication may be preferred whenever possible to offload wearable-generated traffic between the neighboring users and thus avoid the use of a more expensive cellular resource [6]. To this end, D2D connectivity is becoming an effective enabler to reach the target QoS improvements as well as mitigate cellular network congestion within the emerging 5G ecosystem [7].

Broadly, attractive D2D technologies may be divided into two general classes: sharing cellular licenced spectrum or using dedicated resources. The first case tends to be constrained from the power and spectrum management point of view as well as is expensive to use [8], while the second one suffers from uncontrolled interference and offers no QoS guarantees due to the random access behavior of e.g., IEEE 802.11 protocol stack. On the other hand, WiFi provides higher data rates and energy efficiency than cellular technologies [9, 10, 11]. Currently, WiFi is still expected to be the dominant future D2D solution for user device connectivity and thus support wearable aggregation nodes [12].

The range of potential wearable applications in 5G networks is wide. Whenever the users are located in close proximity, they would require respective discovery and identification. Here, D2D connectivity helps disseminate user identification data to facilitate further direct interaction between their connected devices [13]. Proximal connectivity can also assist in retrieving lost connections or locating "familiar strangers" that share similar interests, especially when supplied with relevant social knowledge. On the other hand, collaborative content creation and sharing empower proximate users to opportunistically download and exchange their desired content. Further, D2D-based wearable interaction can assist people in physical proximity to engage jointly into collective activities and communicate with each other's wearable devices with the emphasis on socialization and leisure. This category also includes many location-based services.

Importantly, D2D communications can also serve as a technology component for providing public protection and disaster relief (PPDR) as well as national security and public safety (NSPS) services [14]. More generally, mission-critical services may require very high reliability, ubiquitous coverage, and extremely low latency (needed for e.g., PPDR) [15]. Proximity-based communication has the potential to take its place as an enabling technology in this field [16]. However, effective implementation of this technology with the emphasis on user adoption aspects has to be pursued [17]. Along these lines, information security issues should play the key role, especially given that wearable devices are not only transmitting but also storing personal data that should be processed with due care [18].

Our main goal in this research is to study the novel hybrid centralized/distributed architectures that emerge in close relation to wearable devices. The underlying objective is to enable *secure* data delivery for already communicating D2D users and their associated wearable devices even in the cases of *unreliable* cellular connectivity [15]. The latter may become temporarily unavailable to users due to a variety of different factors, including user mobility, obstacles, etc. When connected to the centralized infrastructure, a group of relevant D2D users (e.g.,

those based on social ties) can straightforwardly establish their own information security rules with conventional methods. However, whenever cellular connection becomes unavailable (unreliable), our proposed framework empowers a certain number of user devices in this group to admit a new (previously unassociated) device or to exclude one of the existing members from the group. Today, such group admission/exclusion can only be managed by the cellular network employing its public key infrastructure, and our proposed protocols *extend* this functionality for the cases of partially unavailable cellular connection (in tunnels, airplanes, elevators, etc.).

The *contributions of this work* are as follows: we discuss our novel information security protocols for network-assisted D2D connectivity utilizing social-aware cluster formation based on a game theoretic approach. To this end, our framework maintains connectivity even when cellular network connection becomes temporarily unavailable. The proposed protocols are embedded into a hierarchical network architecture, where the game theoretic methods are first used to decide upon the preferred user clusterization by exploiting both spatial and social proximity of users. Then, the appropriate information security procedures take these clusters at input to enable secure data exchange within them as well as facilitate cluster joining and leaving procedures. Our numerical results demonstrate that the use of cellular-assisted D2D technology provides substantial gains in terms of secure communication across a number of scenarios and mobility patterns.

This rest of this text is organized as follows. The system model and the structure of the proposed framework are introduced in Section 2. Sections 3 and 4 discuss the game-theoretic clusterization approach and the information security procedures, respectively. Numerical results are provided in Section 5, followed by a Conclusion.

2. Considered system model

In our target scenario, we consider a set of wearable devices and each of these has a wireless connection via a certain radio technology to a more powerful aggregating device. Further, the user smartphone is assumed as the said aggregator that transmits data from wearable devices to the application server in the operator's network [19]. Practically, the mobile smartphone in question may have a number of radio interfaces, including short-range (e.g., BLE, WiFi) and cellular (LTE). In addition, this device is assumed to have a possibility to connect directly to another smartphone over a D2D link. In other words, we consider the second level of abstraction – a type of an *ad hoc* network topology between user mobile phones. Finally, at the highest level of abstraction, there is an infrastructure-based cellular network with all the smartphones connected to it. Detailed overview of the considered architecture may be found in [20].

We name a mobile smartphone with its associated wearable devices as a body area network or a user personal cloud. To this end, user devices belonging to an individual person are assumed to all be trusted nodes. The data circulating between wearables may then be forwarded over the mobile phone's cellular link

to the operator's network and further on to the corresponding application cloud. However, we yield no restrictions on the specific locations of users and some of them might end up being out of cellular coverage. In case of unreliable cellular connection, the needed data can be relayed by other proximate users, whereas the users themselves may move around according to a certain mobility model. It is important to note that in the envisioned scenario the smartphone represents the bottleneck in providing connectivity to the body area network (or user personal cloud). The devices forming the body area network typically have very short-range connectivity (e.g., Bluetooth low-energy) and connect to the Internet through a gateway node, such as the user smartphone in our case.

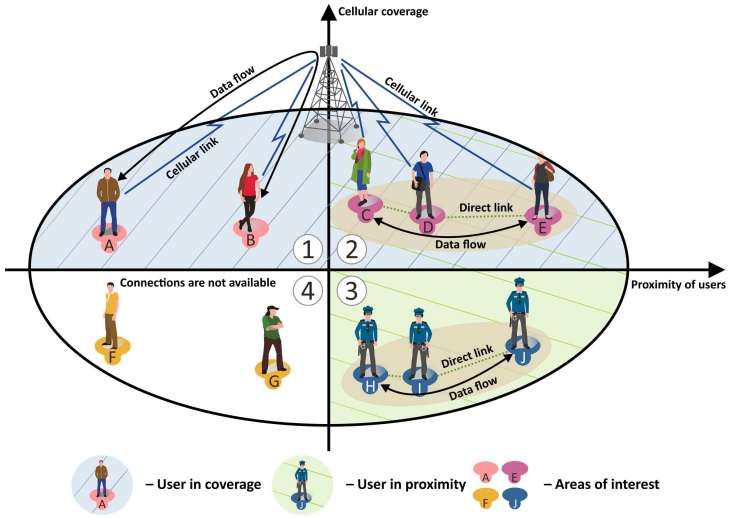


Figure 2: Available D2D system operation modes.

Let us then concentrate on an arbitrary collection of proximate users in our network (i.e., a cluster). Depending on its location, there could be a number of special cases of interest, see Fig. 2. First, the cluster could be fully under the coverage of a cellular BS and conventional information security procedures may be employed to protect data transmitted over the cellular connection to the infrastructure network. In more detail, the first case in Fig. 2 suggests that both security procedures and data flows travel through the base station (BS), while for the second case only security procedures are enabled by the BS (data is exchanged directly between smartphones). In the third case, both security procedures and data flows utilize a direct link among users. Although the proposed framework is designed to embrace all the discussed use cases, the last of the three is of particular interest as it has not been addressed comprehensively in past literature. Enabling proximate users to not only communicate directly in a secure fashion, but also validate their data exchange as they leave and return under the cellular coverage, is one of the main targets of our present research. As a last possible case, the cluster could be fully out of the cellular

network's coverage. In this case, existing ad hoc specific solutions may be utilized to provide continuous secure connectivity for users over their direct links. However, according to the network-assisted D2D concept in beyond 4G systems, the management of the direct link initialization, operation, and destruction is orchestrated by the cellular infrastructure.

Within our proposed framework, depending on the specific application running on top of user personal networks, the resulting clusters are based on two types of proximity-related parameters. First, there is *spatial proximity* of mobile users, which affects the optimal configuration of clusters with respect to wireless channel quality criteria. Optimizing this metric across all the mobile devices, we may improve the data rate performance of the system. The other type of proximity is so-called *social proximity* of users. A mobile device can be aware of its previous contacts with other mobile users, or alternatively this information can be obtained from the contacts already stored on the smartphone. In what follows, we show how this information can be efficiently exploited to improve the performance of the security algorithm introduced later. To this end, the initial clustering of nodes is conducted by utilizing game-theoretic approaches – a subset of classical optimization theory – by efficiently exploiting both spatial and social notions of proximity.

Importantly, the proposed framework takes into account the effects of user mobility. The classical methods of optimization theory consider a *snapshot* of a network at a certain instant of time t and then aim at developing practical algorithms for the optimized system operation with respect to a certain metric of interest. Clearly, such an approach cannot directly incorporate the mobility of users as it may cause significant deviations from the optimal solution at some other time $t+\Delta t$. However, enabling a particular mobility model and performing respective optimization at discrete instants of time, we can implicitly capture the effects of mobility. Finally, the reason behind the use of game theoretic approaches in our mobile user environment is due to the complexity of keeping track of the past device behavior resulting from the high dynamics in these networks [21]. In particular, coalitional game theory is applied to model the cooperative behavior among network devices focusing on the payoff groups of devices, rather than individual devices, as discussed next.

3. Game-theoretic clustering procedure

The selection of a preferred cluster configuration can be modeled as a non-transferable utility (NTU) coalitional game. A coalitional game is defined by the pair $(\mathcal{N}, \mathcal{V})$, where $\mathcal{N}$ is the set of N players and $\mathcal{V}$ is a set valued function, such that for every coalition $\mathcal{S} \subseteq \mathcal{N}$, $\mathcal{V}(\mathcal{S})$ is a closed convex subset of $\mathbb{R}^{|\mathcal{S}|}$. It contains the payoff vectors, which the players in $\mathcal{S}$ can achieve, where $|\mathcal{S}|$ is the number of members in coalition $\mathcal{S}$.

In our model, the players are user smartphones forming a cluster. The game is given in its characteristic form, as the achievable utility within a coalition only depends on the players forming the coalition and not on other players in the network. The objective for the players is to maximize the value of the coalition

that is defined as the degree of geographical proximity and social relationship for the formed cluster. Hence, the coalitional game is an NTU game, since this value cannot be arbitrarily apportioned among players. We define $\mathcal{V} : \mathcal{S} \rightarrow \mathbb{R}^{|\mathcal{S}|}$, such that $\mathcal{V}(\emptyset) = \emptyset$, and for any coalition $\mathcal{S} \subseteq \mathcal{N} \neq \emptyset$ it is a singleton set $\mathcal{V}(\mathcal{S}) = \{\mathbf{v}(\mathcal{S}) \in \mathbb{R}^{|\mathcal{S}|}\}$, where each element of the vector $\mathbf{v}(\mathcal{S})$ is the value $v_i(\mathcal{S})$ associated with each player $i \in \mathcal{S}$. The latter is defined as:

$$v_i(\mathcal{S}) = \frac{\sum_{j=1}^{|\mathcal{S}|} s_{i,j} \cdot d_{i,j}}{|\mathcal{S}|}, \tag{1}$$

where $s_{i,j} \rightarrow [0, 1]$ is an asymmetric function (i.e., $s_{i,j} \neq s_{j,i}$) measuring the social relationship or the degree of *friendship* between two devices. In particular, $s_{i,i}$ is a measure of the willingness of a device to acquire the content over a D2D link from a "friend" instead of directly downloading it from the cellular BS. The second term $d_{i,j}$ is a binary function taking the value of 0 whenever the devices i and j are not in proximity, and the value of 1 otherwise (we set $d_{i,i} = 1$ by construction). The result of the product of these two functions is averaged across the number of players in a given coalition $\mathcal{S}$, which always results in a value within the range $[0, 1]$.

We can now also define the value $v(\mathcal{S})$ associated to a coalition $\mathcal{S}$ as the average spatial and social proximity strength of the devices in a cluster:

$$v(\mathcal{S}) = \frac{\sum_{i=1}^{|\mathcal{S}|} v_i(\mathcal{S})}{|\mathcal{S}|}. \tag{2}$$

In particular, a value $v(\mathcal{S}) = 1$ is obtained when all the devices are within mutual D2D coverage and have the maximum degree of "friendship", so that they are all willing to acquire their desired content from a D2D partner. This seldom happens in larger coalitions, hence smaller independent coalitions are typically formed. Consequently, our proposed approach is modeled after a coalition formation game, with the aim of revealing the network's coalitional structure.

Coalition formation algorithm

Here we assume that all considered devices are rational and autonomous, which substantiates the design of an iterative algorithm to form the network coalition structure that improves both spatial and social proximity of the formed clusters. With respect to alternative scenarios illustrated in Fig. 2, the coalition formation algorithm may be implemented either in a *centralized* or a *distributed* manner. In particular, for *study case 2* represented in Fig. 2, the algorithm will be implemented by the BS (i.e., centralized approach), whereas in *study case 3* the involved devices implement the proposed algorithm autonomously and then synchronize over time by using the beaconing messages to obtain the up-to-date information (i.e., distributed approach). Another alternative for this latter case may become available when at least one of the involved devices is under the

network coverage. In such a case, the BS may still be in charge of the solution implementation, whereas the node under coverage acts as a signaling gateway to the other nodes. However, this latter option may cause some additional signaling overhead.

We define a *collection* of coalitions $\mathcal{C}$ as the set $\mathcal{C} = \{\mathcal{C}_1, \ldots, \mathcal{C}_k\}$ of mutually-disjoint coalitions $\mathcal{C}_i \subset \mathcal{N}$, such that $\mathcal{C}_i \cap \mathcal{C}_{i'} = \emptyset$ for $i \neq i'$. If a collection contains all players in $\mathcal{N}$, i.e., $\bigcup_{i=1}^{k} \mathcal{C}_i = \mathcal{N}$, then the collection is named a *partition* Π or *coalition structure*. Further, the set of all possible partitions of $\mathcal{N}$ has a total number of B_N, where B_N is the N-th Bell number [22], and it grows exponentially with the number of players N. Therefore, obtaining the optimal partition via exhaustive search across all possible partitions is not feasible, as it is an NP-complete problem [23]. An alternative solution is to enable players to join or leave a coalition based on well-defined preferences.

A *preference operator* $\rhd$ 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 $\mathcal{S} \subseteq \mathcal{N}$, so that the same players are involved in the two collections. We say that $\mathcal{L} \rhd \mathcal{Q}$, if the way $\mathcal{L}$ partitions $\mathcal{S}$ 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:

$$\mathcal{L} \rhd \mathcal{Q} \Leftrightarrow \sum_{i=1}^{l} v(\mathcal{L}_i) > \sum_{j=1}^{q} v(\mathcal{Q}_j). \tag{3}$$

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

Definition 1 (Merge Rule). *Merge any collection of disjoint coalitions* $\{\mathcal{C}_1, \ldots, \mathcal{C}_k\}$ *if* $\{\bigcup_{i=1}^{k} \mathcal{C}_i\} \rhd \{\mathcal{C}_1, \ldots, \mathcal{C}_k\}$, *thus* $\{\mathcal{C}_1, \ldots, \mathcal{C}_k\} \rightarrow \{\bigcup_{i=1}^{k} \mathcal{C}_i\}$.

Definition 2 (Split Rule). *Split any coalition* $\{\bigcup_{i=1}^{k} \mathcal{C}_i\}$ *if* $\{\mathcal{C}_1, \ldots, \mathcal{C}_k\} \rhd \{\bigcup_{i=1}^{k} \mathcal{C}_i\}$, *thus* $\{\bigcup_{i=1}^{k} \mathcal{C}_i\} \rightarrow \{\mathcal{C}_1, \ldots, \mathcal{C}_k\}$.

The merge rule implies that two or more coalitions join to form a larger coalition, when operating altogether leads to a greater obtained value than if the coalitions functioned separately. In contrast, the split rule implies that coalitions split into smaller coalitions if this has a positive effect on the total value. As a result, the game is implemented by each individual device in a distributed fashion, as summarized in Algorithm (1).

Specifically, starting from an initial partition $\Pi^{ini}(N) = \mathcal{N} = \{p_1, p_2, \ldots, p_N\}$, each device iteratively applies the merge and split rules considering any pair of

Data: Set of devices $\mathcal{N}$
Result: Coalition structure Π^{fin}
Phase I – Neighbor Discovery:

- Each device discovers its neighboring devices and collects the required information.
- Partition the network by $\Pi^{ini}(N) = \mathcal{N} = \{p_1, p_2, \ldots, p_N\}$.
- Set the current partition as $\Pi^{cur}(N) = \Pi^{ini}(N)$.

Phase II – Coalition Formation:
Coalition formation using merge-and-split rules.
repeat
  repeat
    - make *merge* decisions based on the merge rule.
    - If a *merge* operation is performed, then update the current partition $\Pi^{cur}(N)$.

  until *no merge occurs*;
  repeat
    - make *split* decisions based on the split rule.
    - If a *split* operation is performed, then update the current partition $\Pi^{cur}(N)$.

  until *no split occurs*;
until *neither merge nor split occur*;
Adaptation to the network topology changes (periodic process): Periodically, the algorithm is repeated to allow for the network architecture to adapt to environmental changes.

Algorithm 1: Distributed coalition formation algorithm.

coalitions in the partition. In particular, the merge process stops when no couple of coalitions exists in the current partition $\Pi^{cur}(N)$ that can be merged. Further, the split rule is applied to every coalition in the partition by updating $\Pi^{cur}(N)$ if a split is applied. When no split occurs, the algorithm considers the merge function again. Our proposed algorithm terminates when no merge or split has occurred at the last iteration. In this case, the final resulting partition $\Pi^{fin}(N)$ will be adopted. It can be proved that the final partition established by the proposed merge and split algorithm is *stable*, which corresponds to the equilibrium state in which players do not have incentives to leave the formed coalitions [24]. Moreover, the network structure is adapted to the environmental changes (e.g., due to mobility) by periodically repeating the solution computation. In particular, the update period should be chosen depending on how rapidly the said conditions change and has to be equal across all the involved devices.

4. Information security considerations

4.1. Securing D2D communication

In modern cellular networks, the central control infrastructure that orchestrates the associated wireless devices is typically assumed to be always available. Consequently, given its reliable and ubiquitous presence, cellular network is often chosen to serve as a *trusted authority* for security purposes. In proximity-based D2D communication with continuous cellular connectivity, the cellular BS

may be made responsible for managing security functions within its network, and most of the corresponding operations can thus be handled over the Public Key Infrastructure (PKI) [25]. The main properties of such a system are: (i) network architecture should be based on the PKI; (ii) user should be able to change its PKI-based key easily; (iii) encrypted data should contain information on the session data key for all the authorized users. On the other hand, for wireless architectures not relying on pre-existing infrastructure, communication and security functions can be distributed across users [26, 27].

Although the D2D system operation may, at first glance, appear similar to that of ad hoc networks, there is one key difference allowing relaxation of numerous restrictive assumptions related to "pure" ad hoc topologies. In case of cellular-assisted D2D connectivity, all the communicating devices are also associated with the cellular BS, at least for some time. The BS thus facilitates the 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 scenarios by utilizing the possibility to (occasionally) access the trusted cellular infrastructure.

When designing our security solution, we assume that the cellular network coverage is imperfect and sometimes users can face situations of unreliable cellular connectivity due to natural obstacles, tunnels, planes or other issues. However, while using proximity-based services, such as games, file sharing, and data exchange, the users are assumed to have continuous support for those applications over a secure channel. In order to understand what kind of new functionality is needed for the discussed security procedures, consider the connectivity cases demonstrated in Fig. 2 in more detail. All of the possible scenarios that may appear in a network-assisted D2D system can in principle be reduced to the four cases discussed below.

• *Case 1.* Here, users A and B grouped together have already established their own secure group (i.e., *coalition*) based on their area of interest and are using the cellular connection to the operator's network, the application server, and the PKI. The coalition secret has already been generated at the server side, and the users have all received the corresponding credentials and certificates of each other – they remain connected to the cellular network that orchestrates their data exchange. As a result, the data flows are running over cellular links due to the absence of proximity between the devices.

• *Case 2.* Here, we focus on another set of devices consisting of C and D, as well as E that all have already established a coalition. Then, a *heavy* data flow may be running on the direct link between the devices that does not affect the cellular network capacity. All the needed information security procedures for the coalition establishment and key exchange are performed similarly to *Case 1.*

• *Case 3.* In this case, the coalition does not have an active connection to the cellular network. Hence, all the required key generation and distribution procedures are conducted over the direct D2D connections, by contrast to the previous cases. These procedures require higher involvement of the participating devices. The coalition secret is kept unchanged until the tagged group of the devices regains cellular network coverage.

• *Case 4.* In this case, the users are neither in the cellular coverage nor have a possibility to communicate directly. As a result, no security algorithm needs to be executed and users are waiting for the cellular coverage or direct connection to (re)appear.

4.2. Proposed information security procedures

For the purposes of our security protocol, we assume that the cellular network is a trusted authority (TA) that is responsible for the root certificate generation and validation. Moreover, cellular operators are assumed to be responsible for security, anonymity, and privacy aspects of their users. Each user device thus obtains its own certificate signed by TA as soon as it connects to the cellular network for the first time. This step is required to ensure the validity of other users and prevent from the subsequent person-in-the-middle types of attacks on the direct link. We classify users based on their cellular connection availability as well as the fact of their association to a certain secure group: a *light* device has an active, reliable cellular connection; a *dark* device does not have a reliable cellular connection, but used to have it in the past; a *blank* device is that wishing to join the coalition for the first time. In what follows, we address the crucial procedures of coalition initialization and formation.

The procedure of *coalition initialization* may only be executed when connected to the TA, i.e., having a reliable cellular connection. Accordingly, when the i^{th} user receives its initial certificate (PK_i) signed by the root certificate (PK_{TA}, N_{TA}) and is supplied with a unique device identifier, the corresponding secret (SK_i) is generated on the user side. If a group of *light* users is willing to create/initialize a coalition, one of the devices is sending a request to the TA over its cellular link. The request contains the set of device identifiers to be grouped. When the request is processed, a unicast polling procedure is initialed, that is, all of the devices are contacted as to whether they would like to join the coalition. Then, cellular network proceeds with the initial setup of the coalition based on the received responses and according to classical PKI mechanisms. For each initialized secure group, its own coalition certificate (PK_c, PK_{TA}) is generated with the corresponding signature by each device's certificate in the group (PK_i, PK_c). After these initial steps, secure direct communication becomes possible over any IP-ready network. However, the above coalition establishment procedure may only be executed when all of the devices have reliable cellular connectivity due to the protocol constraints.

After the secure coalition has been established, users need not rely on continuous cellular connectivity and may communicate directly over a secure channel even if the cellular link becomes unavailable. However, this type of connectivity can be significantly augmented by offering a possibility to include new users and exclude existing ones from the tagged coalition. Such scenarios may appear in both considered cases: (i) when all the users are *light* – they have cellular connectivity and (ii) when at least one user is *dark* – does not have a reliable cellular connection. These cases correspond to two distinct network operation modes (namely, infrastructure and ad hoc), and the respective security enablers

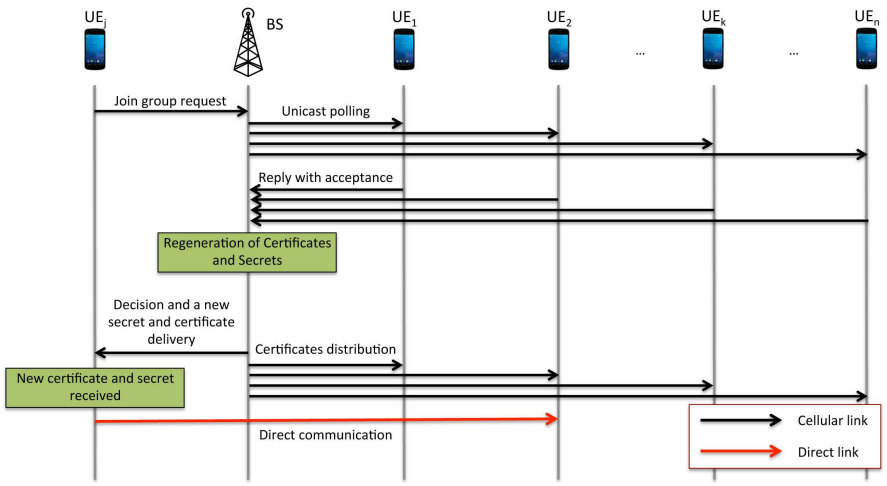


Figure 3: Protocol operation in case of *reliable* cellular connectivity.

for both of them need to be different. The information security procedures for these two scenarios are described as follows.

• *Reliable cellular connectivity.* First, we describe how the initialization of the coalition is performed. All of the devices have a pre-generated set of parameters after their initial network entry: (i) own secret SK_i, (ii) own certificate signed by the TA certificate PK_i, PK_{TA}, and (iii) own unique identifier ID_i. Further, after the TA polls the involved devices and receives a list of users to be grouped, it generates a polynomial $f(x) = a_{k-1}x^{k-1} + a_{k-2}x^{k-2} + ... + a_1x + SK_c$, $f(0) = SK_c$, where k is a threshold value calculated based on the number of devices in the planned coalition, x_i is the device identifier, and a_i is the corresponding device coefficient. Therefore, the RSA-like certificate component for the j^{th} device is calculated as $cert_j = \overline{PK_i}^{f(0)} mod\, N_c$, where $\overline{PK_i}$ is generated by the device, $f(0)$ is the coalition secret, and N_c is generated at the coalition initialization stage as well. Finally, all the certificates are distributed to the devices, and the algorithm proceeds to the phase of direct communication. The above procedure is managed by the TA, whereas the process is illustrated in Fig. 3.

• *Unreliable cellular connectivity.* Focusing on the worst-case scenario, when none of the devices have an active cellular connection, the users should rely only on the coalition itself, when admitting an additional user. To solve this issue, we employ a dedicated parameter included into the coalition certificate PK_c, which is a threshold value of k that characterizes the number of devices in coalition needed to collectively allow for a new device to join in. The value of k is first set at the coalition initialization stage and may then be altered based on the number of involved devices n. Originally, for each coalition, the TA generates a Lagrange polynomial sequence with k coefficients and a coalition secret share

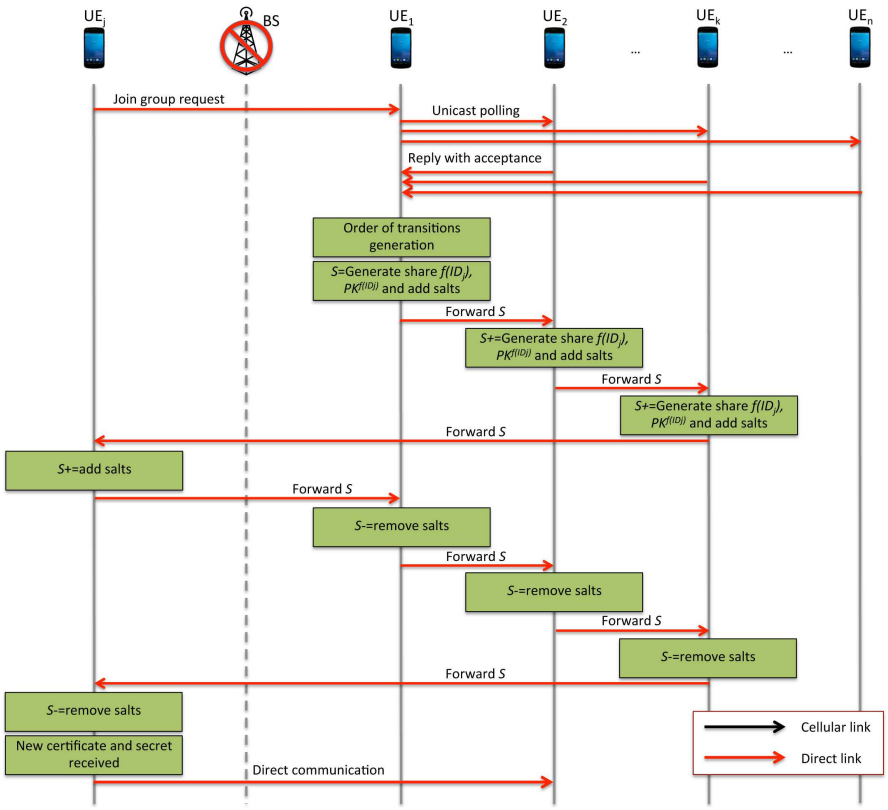
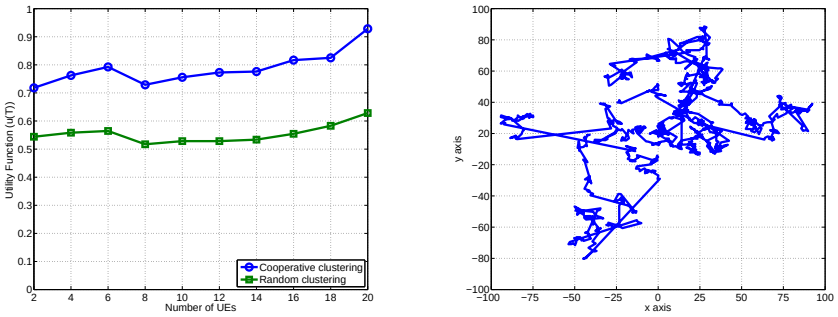


Figure 4: Protocol operation in case of *unreliable* cellular connectivity.

SK_c stored at the cellular network side. Note that for the considered ad hoc scenario, a modification of the polynomial and its associated secret is not possible. Therefore, a group of devices forming the existing coalition should convene together and reconstruct SK_c (without disclosing it) in order to admit the new device, as demonstrated in Fig. 4. Clearly, the same procedure executed without cellular network assistance would cause users to exchange excessive amounts of signaling messages in addition to running computationally intensive information security primitives. On the other hand, with our proposed procedure, secure direct connectivity enjoys higher flexibility and has lower overhead.

5. System-level performance evaluation

In this section, we evaluate the performance of our proposed framework. First, recalling the structure of the discussed framework as a combination of the game theoretic clusterization and the information security procedures, we assess



(a) Comparison of the average individual user equipment (UE) utility

(b) A sample user movement pattern with Levy Flight mobility model

Figure 5: Average user utility varying the number of UEs and Levy Flight model example.

their individual operation in subsections 5.1 and 5.3, respectively. Complexity-related aspects are discussed in subsection 5.2. Then, in subsection 5.4, we employ our large-scale system-level simulator to yield numerical conclusions on the operation of the complete system.

5.1. Analyzing our game theoretic approach

We employ our game theoretic mechanisms in MATLAB and define a square network area of $[100, 100]$m with a varying number of users that are uniformly distributed within this area. In particular, the number of users varies from 2 to 20 and their proximity to each other is characterized by a parameter named $d_{i,j}$, which is equal to "1" when a generic user i is in proximity to a generic user j, and "0" otherwise. In particular, the maximum suitable range for a D2D transmission is set to 30m. In this network, all the users are involved into social relationships among each other and the level of "friendship" between a generic user i and a generic user j is characterized with the *social contact* value $s_{i,j}$. In addition, the social contact value between a generic user i with him-/herself (i.e., $s_{i,i}$) represents the willingness to acquire the desired content via the cellular link. In our considered scenario, the strength of the social relationships among users is modeled according to a uniform distribution in the range $[0, 1]$. Generally, 0 corresponds to two unfamiliar users (e.g., have never met each other) and 1 is the maximum achievable value for the social proximity.

Fig. 5(a) shows the value of the utility function introduced in Section 3, when the devices are clustered with the proposed game theoretic cooperative mechanism compared against a random clusterization. As we can notice, the average utility function per user increases linearly with the number of users. In particular, cooperative clustering achieves a gain of up to 45% (maximum is attained at 12 users) compared to the random clustering. This is explained by the fact that, as the number of users increases, the probability to identify a suitable candidate to form a coalition grows.

5.2. Complexity analysis

Finding the optimal partition requires iterating over all the possible partitions in a given set of users (in our case, in the range $[2, 20]$), which is not feasible, as it is an NP-complete problem [23]. Indeed, the number of possible partitions typically grows exponentially with the overall number of users and is characterized by the Bell number [22]. In the reference problem, however, not all coalitions are feasible and these can be excluded from the search space reducing the overall complexity. In particular, whenever the distance between two users does not allow for a D2D link to be formed (i.e., $d_{i,j} = 0$ in eq. (1)), the corresponding coalition can be excluded from the search space (for more details on this please refer to the constrained coalition formation game in [28]). Given the search space for our problem at hand, the game theoretic coalition formation algorithm allows to reduce the complexity. In fact, the complexity of a single mechanism iteration for the proposed game theoretic scheme is defined by the number of iterations performed by the merge and split attempts multiplied by the complexity of the utility function described in (2). In particular, starting from the initial partition with e.g., m coalitions, in the worst case the first merge step occurs after $m(m-1)/2$ attempts, while the second one requires $(m-1)(m-2)/2$ attempts, etc. As a result, in the worst case the number of merge attempts is in $O(m^3)$. However, in practice the merge operation requires a significantly lower number of attempts as once the two coalitions are merged the mechanism will not go further in the m possible coalitions space.

For the splitting operation, this can imply finding all the possible partitions of size 2 for each coalition S in the current network partition. Therefore, the split operation is restricted by the number of users inside the coalition S and not by the total number of possible coalitions m. Implicitly, the split operation is limited to the already formed coalitions (after the merge process has been performed), which generally do not represent the grand coalition (i.e., a single coalition formed by all the users). Moreover, the complexity is further reduced in a practical setting where it is not required to go through all the split forms. As soon as a coalition finds a split form, the user equipments (UEs) in this coalition will split, and the search for further split forms will not be required.

To provide a quantitative analysis of the computational complexity for the proposed cluster formation approach in Table 1, we report information on the obtained numerical results for a test case with different numbers of users in the network. Given the D2D link coverage constraints and the corresponding possible coalitions to form in the network, we offer the number of iterations, the coalition size, and the search space size for the proposed game theoretic vs. the exhaustive search solutions. As one can notice, in the worst situation (i.e., 20 users) the actual partitions are 260 compared to $5 \cdot 10^{13}$ available partitions reached with the exhaustive search. Note that a reduced number of operations also means a lower execution time.

5.3. Analyzing our information security procedures

In this subsection, we discuss the critical components of the proposed information security framework. Recall that even though our secure group ini-

Table 1: Numerical results for the cluster formation solution

Users	Coalition size [# UEs]	# of iterations	Game theory [search space size]	Exhaustive search [search space size]
2	2	1	2	2
4	2	3	6	15
6	2	4	8	$2 \cdot 10^2$
8	3	5	25	$4 \cdot 10^3$
10	3	5	25	$1 \cdot 10^5$
12	4	5	75	$4 \cdot 10^6$
14	4	5	75	$1 \cdot 10^8$
16	5	5	260	$1 \cdot 10^{10}$
18	5	5	260	$6 \cdot 10^{11}$
20	5	5	260	$5 \cdot 10^{13}$

tialization can only be performed under cellular network coverage, the users in the existing coalition can include/exclude other users in two different ways, depending on the availability of the cellular link. These examples are discussed in detail further on.

One of the important aspects of the proposed security-centric framework is the performance of the coalition joining procedure. We distinguish between D2D built over WiFi-Direct and LTE-Direct technologies. The delay when joining the coalition over LTE-Direct, as we use unicast methods for user request processing, that is, all of the polled devices have to reply, is given by:

$$T = L_{U \to BS} + nL_{BS \to U} + nL_{U \to BS} + L(t^{f(x)}) + (n+1)L_{U \to BS}, \qquad (4)$$

where n is the number of devices in a coalition, $L_{U \to BS}$ is the time needed to send a message from a cellular user to the cellular BS, $L_{BS \to U}$ is the time needed to receive a response from the BS, $L(t^{f(x)})$ is the time to generate the polynomial sequence, certificates, and keys by the cellular network.

Similarly, for WiFi-Direct based D2D implementation we have:

$$T = 3W_{U_j} + 2nW_{U_i} + W(t^p) + k(W_{U_i} + t^s + t^r) + t^r + k(W_{U_i} + t^{-r}) + t^{-r}, \quad (5)$$

where k is a threshold value equal to the number users needed to include/exclude another one, W_{U_j} is the time needed to communicate between a coalition and a new user, W_{U_i} is the time for communication between two users inside the coalition, $W(t^p)$ is the time to complete all the protocol execution steps, t^s is the time to generate a share on the user side, as well as t^r and t^{-r} are the times to add and remove cryptographic "salts".

To evaluate the operation of our information security framework, we have performed tests in a real-life environment. For the server side, we employed the CentOs virtual machine [29] with two virtual processors Intel(R) Xeon(R) CPU

X5472 both running 3.00GHz, 6MB cache size. As a mobile device, we have chosen a Jolla smartphone [30] running Sailfish OS with Qualcomm Snapdragon 400 1.4 GHz dual-core processor (8930AA). The comparison of the experimental results for the RSA algorithm using OpenSSL [31] is summarized in Table 2. We confirm that the larger the key is, the longer it takes to compute the primitives. The results obtained with a more powerful server-side processor are approximately 10 times better than those obtained on the user side, as it is shown in Table 2. In this study, we use standard software library available on most of the mobile devices, implying that the results can be improved by utilizing specialized lightweight cryptography and hardware on-chip solutions.

Table 2: Security primitives: execution time.

Primitive	Server, μs	Mobile Device, μs
RSA 512 public key	7.28	109.32
RSA 512 private key	99.95	1157.80
RSA 1024 public key	19.57	305.81
RSA 1024 private key	352.38	5991.61
RSA 2048 public key	66.83	953.56
RSA 2048 private key	2158.89	35987
Random variable generation	7.23	24.95

5.4. Selected simulation results

To evaluate the performance of the proposed information security approach summarized in Section 4, a simulation-based campaign has been conducted using the WINTERsim tool available in [32]. The reference scenario consists of a 3GPP LTE BS (termed eNodeB) with the radius of 100m, where users are uniformly distributed within its coverage in the range $[10, 100]$. The movements of the users are characterized by a *Levy Flight* mobility model with an α-value equal to 1.5 and the user speed varying in the range $[0.2, 2.0]$m/s. An example of user mobility pattern is illustrated in Fig. 5(b). The reason for choosing the Levy Flight mobility model is that recent investigations reveal that movement of people may follow characteristic patterns, where numerous short runs are interchanged with occasional long-distance travels [33, 34, 35]. The parameter α allows adjusting the form of the step-size distributions.

Importantly, in our reference scenario the connection between the smartphone and the devices within the user personal cloud is assumed to be trusted and stable. In particular, with our simulation-based evaluation the focus is on the smartphone which represents a bottleneck for providing stable and secure communication to the entire personal cloud (wearables). Indeed, whenever the cellular connection becomes unavailable (unreliable), the proposed solution is able to offer a connection also to the device that is not in network coverage when in proximity to another device.

The simulation environment thus translates into a typical pedestrian scenario, as standardized in the 3GPP specification TS 36.304 (see Section 5.2.4.3

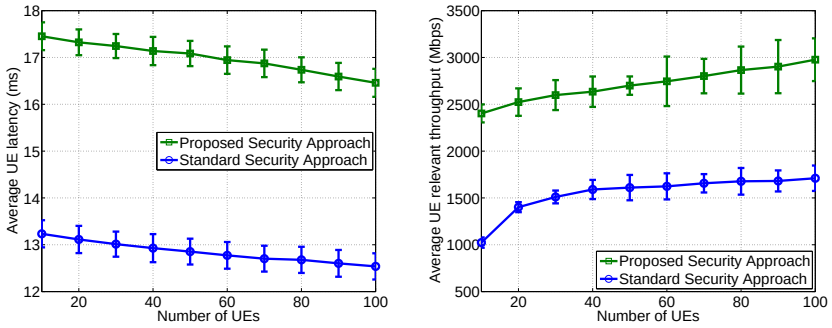
therein). In addition, the multimedia traffic within the considered scenario is modeled after a video download application with relatively long inter-arrival time and the packet size of 100MB. The main system parameters are summarized in Table 3. The two performance metrics that we focus on are: *user latency*, that is, the end-to-end delay to download the multimedia content, *average user relevant throughput*, that is, the throughput achieved by the UE when it downloads the desired content either over the LTE or the WiFi-Direct link, and *blocking probability*, that is, the number of interruptions experienced by the user during a download session. We compare the conventional network operation against the security-centric approach outlined in Section 4.

Table 3: The main simulation parameters.

Parameter	**Value**
Cell radius	100 m
Maximum D2D range	30 m
# of users	20
Target data rate on LTE link	10 Mbps
Target data rate on D2D link	40 Mbps
eNodeB Tx power	46 dBm
UE Tx power	23 dBm
D2D link setup	1 s
Cellular bandwidth	5 MHz
Mobility model	Levy Flight
Simulation time	15 min
Number of simulation runs	300

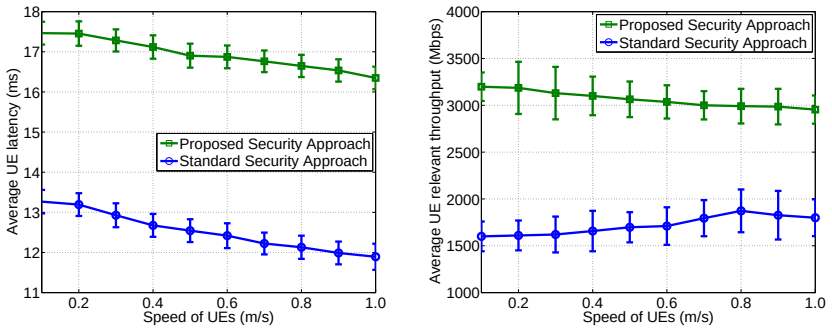
First, consider the effects of user mobility on the average latency in the proposed framework (see Fig. 6(a) and Fig. 7(a)). As we can observe, the latency decreases linearly with the growing intensity of mobility either by varying the number of users or the mobility intensity. The reason is that the increase in the user speed translates into higher number of contacts among them. This way, users can download the content over the WiFi-Direct link with higher data rates. However, the conventional security approach performs better compared to the proposed solution. This is due to the fact that our security scheme introduces an additional delay when users are in proximity (can establish a direct D2D connection), but not under the network coverage, i.e., *Case 3* in Fig. 2. This effect is particularly visible when the number of users is high (i.e., 100), because the opportunities to establish direct connections become more abundant. However, the advantage of using our approach is in that, generally, conventional systems are unable to provide any type of secure connectivity when there is a lack of cellular coverage.

The average throughput experienced by the users as a function of the number of UEs and their mobility intensity is shown in Fig. 6(b) and Fig. 7(b). It is important to note that the proposed security algorithm demonstrates better performance compared to the conventional solution. The reason is that our approach delivers connectivity to users that are in a D2D transmission range, but not under cellular coverage, *Case 3* in Fig. 2. In this case, the *extra* throughput



(a) Average user latency (b) Average user relevant throughput

Figure 6: Latency and throughput for varying number of UEs (speed is 1 m/s).

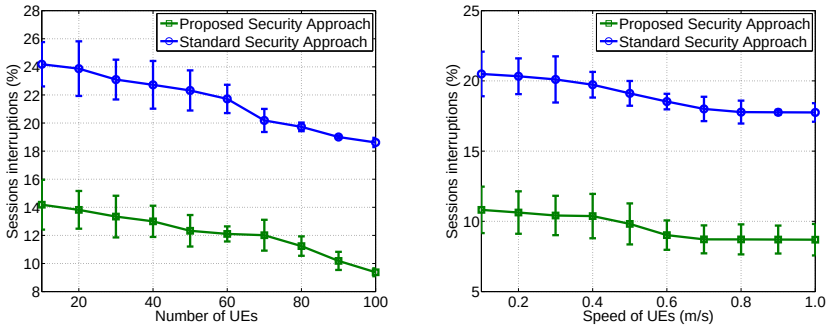


(a) Average user latency (b) Average user relevant throughput

Figure 7: Latency and throughput for varying UE speeds (number of UEs is 100).

is obtained at a cost of additional delay to establish a direct D2D connection and execute all the needed security procedures. The amount of the additional delay is due to execution of the security primitives that have to be run among the D2D users as reported in Table 2.

Finally, the blocking probability as a function of the number of interrupted download sessions experienced by the users is summarized in Fig. 8(a) and Fig. 8(b). As we learn from the plots, the proposed security approach performs better compared to the conventional security solution. The explanation is again that the proposed framework is able to guarantee connectivity even if the users are not under network coverage (i.e., *Case 3* in Fig. 2). As a consequence, at the cost of extra delay, the users enjoy longer download sessions and increase their chances to obtain the desired multimedia content.



(a) Blocking probability for varying the number of UEs

(b) Blocking probability for varying the speed of UEs

Figure 8: Blocking probability.

6. Concluding Remarks

In this paper, we discussed a security framework for proximity services in order to provide additional coverage for users that are facing intermittent cellular connectivity. We exploited a game theoretical framework (i.e., in terms of the cluster formation), where social relationships among users and the effects of cellular transmissions are considered explicitly.

In the reference scenario, we studied the case of the cellular BS providing partial coverage and helping disseminate certain content that has to be distributed among all the active users. In such a situation, the cluster formation game is utilized for the user clustering by employing either social or spatial proximity, whereas the information security procedures take advantage of the obtained group configuration to exchange the data in a protected way.

The obtained results indicated that, even though the amount of signaling messages was slightly increased, the proposed security framework was able to deliver connectivity to those users that were outside the cellular network coverage, and consequently did not have a reliable connection to the cellular infrastructure. As a result, we can assert that the consideration of both network geometry and social metrics enables dissemination of information to larger numbers of users with higher throughput, but at the cost of some additional delay due to extra signaling messages exchanged locally within each cluster.

In summary, we conclude that the proposed framework based on spatial and social notions of proximity significantly improves many performance metrics of interest in characteristic cellular-assisted D2D scenarios, where users exchange traffic generated by their wearable devices while utilizing smartphones as data aggregators. Our modeling approach may thus become useful as a reference point for further research in this field.

Acknowledgment

This work is supported by the Academy of Finland. The work of S. Andreev is supported with a Postdoctoral researcher grant from the Academy of Finland, as well as with a Jorma Ollila grant by Nokia Foundation.

References

[1] Ericsson AB, Ericsson mobility report: On the pulse of the Networked Society (July 2015).

[2] Ericsson LM, More than 50 billion connected devices, White Paper (2011).

[3] M. Billinghurst, T. Starner, Wearable devices: new ways to manage information, Computer 32 (1) (1999) 57–64.

[4] R. R. Fletcher, K. Dobson, M. S. Goodwin, H. Eydgahi, O. Wilder-Smith, D. Fernholz, Y. Kuboyama, E. B. Hedman, M.-Z. Poh, R. W. Picard, iCalm: Wearable sensor and network architecture for wirelessly communicating and logging autonomic activity, IEEE Transactions on Information Technology in Biomedicine 14 (2) (2010) 215–223.

[5] A. Pyattaev, K. Johnsson, S. Andreev, Y. Koucheryavy, Communication Challenges in High-Density Deployments of Wearable Wireless Devices, IEEE Wireless Communications Magazine 22 (1) (2015) 12–18.

[6] L. Militano, M. Condoluci, G. Araniti, A. Molinaro, A. Iera, When D2D communication improves group oriented services in beyond 4G networks, Wireless Networks 21 (4) (2014) 1363–1377.

[7] C.-H. Yu, K. Doppler, C. B. Ribeiro, O. Tirkkonen, Resource sharing optimization for device-to-device communication underlaying cellular networks, IEEE Transactions on Wireless Communications 10 (8) (2011) 2752–2763.

[8] S.-P. Yeh, S. Talwar, G. Wu, N. Himayat, K. Johnsson, Capacity and coverage enhancement in heterogeneous networks, IEEE Wireless Communications 18 (3) (2011) 32–38.

[9] S. Andreev, Y. Koucheryavy, N. Himayat, P. Gonchukov, A. Turlikov, Active-mode power optimization in OFDMA-based wireless networks, in: Proc. of GLOBECOM Workshops (GC Wkshps), IEEE, 2010, pp. 799–803.

[10] C. Sankaran, Data offloading techniques in 3GPP Rel-10 networks: A tutorial, IEEE Communications Magazine 50 (6) (2012) 46–53.

[11] S. Andreev, P. Gonchukov, N. Himayat, Y. Koucheryavy, A. Turlikov, Energy efficient communications for future broadband cellular networks, Computer Communications 35 (14) (2012) 1662–1671.

[12] L. Al-Kanj, Z. Dawy, W. Saad, E. Kutanoglu, Energy-aware cooperative content distribution over wireless networks: Optimized and distributed approaches, IEEE Transactions on Vehicular Technology 62 (8) (2013) 3828–3847.

[13] G. Fodor, E. Dahlman, G. Mildh, S. Parkvall, N. Reider, G. Miklós, Z. Turányi, Design aspects of network assisted Device-to-Device communications, IEEE Communications Magazine 50 (3) (2012) 170–177.

[14] G. Baldini, S. Karanasios, D. Allen, F. Vergari, Survey of wireless communication technologies for public safety, Communications Surveys & Tutorials 16 (2) (2014) 619–641.

[15] G. Fodor, S. Parkvall, S. Sorrentino, P. Wallentin, Q. Lu, N. Brahmi, Device-to-Device Communications for National Security and Public Safety, IEEE Access (2014) 1510–1520.

[16] F. H. Fitzek, M. Katz, Q. Zhang, Cellular controlled short-range communication for cooperative P2P networking, Wireless Personal Communications 48 (1) (2009) 141–155.

[17] P. E. Pedersen, L. B. Methlie, H. Thorbjornsen, Understanding mobile commerce end-user adoption: a triangulation perspective and suggestions for an exploratory service evaluation framework, in: Proc. of 35th Annual Hawaii International Conference on System Sciences. HICSS., IEEE, 2002, pp. 8–pp.

[18] J. Lindström, Security challenges for wearable computing-a case study, in: Proc. of 4th International Forum on Applied Wearable Computing (IFAWC), VDE, 2007, pp. 1–8.

[19] A. Ometov, P. Masek, L. Malina, R. Florea, J. Hosek, S. Andreev, J. Hajny, J. Niutanen, Y. Koucheryavy, Feasibility Characterization of Cryptographic Primitives for Constrained (Wearable) IoT Devices, in: Proc. of International Conference on Pervasive Computing and Communications (PerCom), IEEE, 2016, pp. 1–23.

[20] S. Andreev, D. Moltchanov, O. Galinina, A. Pyattaev, A. Ometov, Y. Koucheryavy, Network-Assisted Device-to-Device Connectivity: Contemporary Vision and Open Challenges, in: Proc. of 21th European Wireless Conference, VDE, 2015, pp. 1–8.

[21] D. Moltchanov, Y. Koucheryavy, J. Harju, Simple, accurate and computationally efficient wireless channel modeling algorithm, in: Wired/Wireless Internet Communications, Springer, 2005, pp. 234–245.

[22] D. E. Knuth, The Art of Computer Programming, Volume 4, Combinatorial Algorithms, Part 1, Addison-Wesley Professional, 2011.

[23] T. Sandholm, K. Larson, M. Andersson, O. Shehory, F. Tohmé, Coalition structure generation with worst case guarantees, Artificial Intelligence 111 (1) (1999) 209–238.

[24] K. R. Apt, A. Witzel, A generic approach to coalition formation, International Game Theory Review 11 (03) (2009) 347–367.

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

[26] Z. J. Haas, J. Deng, B. Liang, P. Papadimitratos, S. Sajama, Wireless ad hoc networks, Encyclopedia of Telecommunications (2002).

[27] M. N. Johnstone, R. Thompson, Security aspects of military sensor-based defence systems, in: Proc. of 12th IEEE International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom), IEEE, 2013, pp. 302–309.

[28] L. Militano, A. Orsino, G. Araniti, A. Molinaro, A. Iera, A Constrained Coalition Formation Game for Multihop D2D Content Uploading, Wireless Communications, IEEE Transactions on PP (99) (2015) 1–1. doi:10.1109/TWC.2015.2497682.

[29] C. Negus, T. Boronczyk, CentOS Bible, Wiley Publishing, 2009.

[30] Jolla smartphone – specification, `https://jolla.com/jolla` (July 2015).

[31] J. Viega, M. Messier, P. Chandra, Network Security with OpenSSL: Cryptography for Secure Communications, "O'Reilly Media, Inc.", 2002.

[32] WINTERsim system-level simulator description, `http://winter-group.net/downloads/` (January 2016).

[33] D. Brockmann, L. Hufnagel, T. Geisel, The scaling laws of human travel, Nature 439 (2006) 462—465.

[34] M. Gonzalez, C. Hidalgo, A. Barabasi, Understanding individual human mobility patterns, Nature 453 (2008) 779—782.

[35] I. Rhee, M. Shin, S. Hong, K. Lee, S. Chong, On the Levy walk nature of human mobility, in: Proc. of INCOCOM 2008, Phoenix, AZ, April 2008, 2008, pp. 276–279.