TAMPEREEN TEKNILLINEN YLIOPISTO
TAMPERE UNIVERSITY OF TECHNOLOGY

ALEKSANDR OMETOV

ENABLING SECURE DIRECT CONNECTIVITY UNDER INTERMITTENT CELLULAR NETWORK ASSISTANCE

Master of Science thesis

Examiners: Prof. Yevgeni Koucheryavy
and
Dr. Sergey Andreev
Examiners and topic approved by the Faculty Council of Faculty of
Electronics and Communications Engineering
on 8th June 2016

ABSTRACT

ALEKSANDR OMETOV: ENABLING SECURE DIRECT CONNECTIVITY UNDER INTERMITTENT CELLULAR NETWORK ASSISTANCE
Tampere University of Technology
Master of Science thesis, 66 pages
September 2016
Master's Degree Programme in Information Technology
Major: Communication Systems and Networks
Examiners: Prof. Yevgeni Koucheryavy and Dr. Sergey Andreev
Keywords: wireless networks, direct communications, proximity, information security, prototyping, performance evaluation

This work targets at investigating direct communications as a promising technology for the next-generation 5G wireless ecosystem that improves the degrees of spatial reuse and creates new opportunities for users in proximity. While direct connectivity has originally emerged as a technology enabler for public safety services, it is likely to remain in the heart of the 5G ecosystem by spawning a wide diversity of proximate applications and services. Direct communications couples together the centralized and the distributed network architectures, and as such requires respective enablers for secure, private, and trusted data exchange especially when cellular control link is not available at all times. Within the research group, the author was tasked to provide the state-of-the-art technology overview and to propose a novel algorithm for maintaining security functions of proximate devices in case of unreliable cellular connectivity, whenever a new device joins the secure group of users or an existing device leaves it. The proposed solution and its rigorous practical implementation detailed in this work open door to a new generation of secure proximity-based services and applications in future wireless communications systems.

PREFACE

This thesis concludes a long-going research on secure direct communications by W.I.N.T.E.R. group at the Department of Electronics and Communications Engineering, Tampere University of Technology (TUT), Finland.

First and foremost, I would like to express my sincere gratitude to my supervisor, Dr. Sergey Andreev, whose expertise and motivation added considerable value to my development not only at the University but also in my personal life.

I would also like to acknowledge our Lab head, Prof. Yevgeni Koucheryavy, for making our lives easier. I am grateful to my colleagues at TUT for their valuable support, patience, and guidance, in particular, to Dr. Alexander Pyattaev and Dr. Olga Galinina.
I would like to extend my acknowledgments to Prof. Sergey Bezzateev from St. Petersburg State University of Aerospace Instrumentation for his help and advices while working on information security issues.
My sincere thanks go to Dr. Jiří Hošek, Pavel Mašek as well as Antonino Orsino from Brno University of Technology and Mediterranean University of Reggio Calabria, respectively, for showing completely different style of work and valuable collaboration.

I would also like to give my special appreciation to people who really care about me: Adam Surák and Roman Florea. Without their support, acceptance, and bad:c0ff:ee, my progress would have never been as strong.

I would like to express my deepest feelings to my family and beloved for never letting me down, for believing in me, and for unconditional love which kept me warm over long Finnish winters.

This work was supported in part by the Academy of Finland, project "Empowering Secure, Private, and Trusted Network-Assisted Device-to-Device Communication".

Tampere, 19.08.2016
Aleksandr Ometov

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

LIST OF ABBREVIATIONS

3GPP	The 3rd Generation Partnership Project
5G	5th Generation
AP	Access point
BLE	Bluetooth Low Energy
BS	Base Station
D2D	Device-to-Device
DHCP	Dynamic Host Configuration Protocol
DL	Downlink
EPC	Evolved Packet Core
IEEE	Institute of Electrical and Electronics Engineers
ISM	Industrial, Scientific, and Medical
IS	Information Security
IoT	Internet of Things
IrDA	Infrared Data Association
LTE	Long Term Evolution
MIMO	Multiple-Input and Multiple-Output
MK	Master Key
P2P	Peer-to-Peer
PGP	Pretty Good Privacy
PKG	Private Key Generator
PKI	Public Key Infrastructure
PWK	Pair Wise Key
QoE	Qialuty of Experience
QoS	Quality of Service
RAN	Radio Access Network
RAT	Radio Access Technology
RSA	Ron Rivest, Adi Shamir, and Leonard Adleman cryptosystem
SIM	Subscriber Identity Module
SINR	Signal-to-Interference-Plus-Noise Ratio
SLS	System-level Simulator
TA	Trusted Authority
UE	User Equipment
UL	Uplink

WLAN	Wireless Local Area Network
WiFi	Wireless Fidelity
WiGig	Wireless Gigabit
eNodeB	Evolved Node B

LIST OF SYMBOLS

ID_i	Unique i^{th} device identifier
MK	Masker key
K	Key set
n	Number of devices
k	Threshold number of devices
i, j	Array indices
PK_{TR}	Trusted authority (root) certificate
N_{TR}	Modulus
PK_i, SK_i	Device public and secret keys
PK_C	Coalition public key
SK_C	Coalition secret
$cert_i$	User certificate
a_{k-1}, b_{k-1}	Lagrange polynomial coefficients
Δ_i	Scaling coefficient for Lagrange polynomial
x^{k-1}	Lagrange polynomial share
s_j	Salt
φ	Euler's formula

1. INTRODUCTION

In recent years, we have been witnessing the proliferation of bandwidth-hungry user applications, which are becoming ubiquitous in the form of multimedia services, interactive games, and social networking solutions [1]. To effectively cope with the resulting avalanche of mobile traffic, fifth generation (5G) networks demand innovative technologies capable of supporting the ambitious system requirements. To this end, unprecedentedly high targets were set for the 5G system design, such as seamless wide-area coverage (with 100 Mbps user rate) and extremely high-capacity hot-spot access (1 to around 10 Gbps user rate). Among the candidate 5G technologies, direct device-to-device (D2D) communications attracts an increased research attention [2] as it promises to deliver improved throughputs, provide more efficient spatial reuse, lead to extended network coverage, and enhance user energy efficiency. Broadly, D2D communications refers to a radio technology that enables devices to communicate directly with each other, that is, without routing the data paths through a network infrastructure.

With the widespread adoption of D2D communications, we expect the user devices to take a more active part in 5G service provisioning and, in some cases (e.g., in partial coverage situations), even assume some of the roles of the network infrastructure. In particular, they can aid in providing wireless connectivity such as offering D2D-based data relaying, proximity gaming, content distribution and caching, and other forms of cooperative communications. This paradigm shift from the conventional cellular model is driven by the natural progress in communications technologies: the user devices are decisively augmenting their capabilities, whereas the base stations (BSs) are becoming smaller as a result of the ongoing network densification [3]. Consequently, the original functional disparity between these key components of the maturing 5G ecosystem – the user equipment (UE) and the BS infrastructure – is gradually becoming blurred.

However, there remains a fundamental difference between the UE and the BS, which is rooted in the ownership rights of the corresponding equipment. Hence, cellular operators may become interested in employing user devices as an important asset in their networks, to benefit from their improved computational power, storage and caching capacity, wireless access and sensing capability, as well as efficient support for proximity services. Accordingly, adequate sources of motivation that facilitate the end-user decisions to lend their personal devices for the collective tasks need to be involved. In return, to compensate for the corresponding reduction in the networking and computation power actually available to the individual user, more powerful network assistance protocols will have to be developed – guiding the UE toward the best opportunities to receive its desired service (e.g., user-in-the-loop [4] and similar concepts). This rationale brings into focus the role that social relations and interactions between an individual human user and its proximate neighbors may play in supporting the maturing D2D communications paradigm.

In the past, community-centric incentives were exploited frequently, which meant agreeing to engage into direct connectivity to cooperate with other like-minded individuals in certain well-defined scenarios (such as a conference, concert, sports match, etc.). However, in order for this solution to scale to network-wide applications, operator-driven incentive mechanisms are strongly demanded. These may e.g., be based on dynamic pricing techniques, as has been proposed in [5]. Indeed, recent D2D-centric studies are already exploring benefits from the integration of social and communications domains [6], but most existing work implicitly assumes that all the users are equally likely to cooperate and share data. However, this is not the case in practice as users acquire and own digital content based on their individual interests and may not be willing to expose it unless trust is established with the D2D partner. As a result, the main motivation behind this research is a possibility to construct a 5G-grade secure D2D connectivity environment featuring both reliable (infrastructure) and intermittent (out-of-coverage) device interactions.

The main goals of this work are as following. The author aims to provide a reliable connection establishment control algorithm; an adaptive mechanism for rapid response to network topology changes or node failures; and an algorithm enabling continuous secure connectivity even when the cellular base station is not accessible.

The thesis is organized as follows. The author firstly presents a technological overview of the network-assisted technology and the corresponding challenges in Chapter 2. The background Chapter 3 provides insight into intermittent connectivity issues within the modern cellular networks and justifies our choices in terms of protocol design. After that in Chapter 4 we formally define the information security mechanism allowing continuous support for secure direct group communications. Chapter 5 is devoted to the performance evaluation study utilizing system-level simulations as well as discusses the corresponding results. Next, in Chapter 6 the implementation of the proposed mechanism in live LTE core is presented. Chapter 7 sheds light on future applications of the direct network-assisted communications and on the standardization aspects of the previously discussed approaches. The last Chapter concludes this thesis work.

2. TECHNOLOGY AND MOTIVATION

Currently, the lion's share of the expected mobile traffic growth comes from peer-to-peer (P2P) services that naturally involve *clients in close proximity* [7, 8] (see Figure 2.1). The potential proximity-based communications also enable shorter and lower-to-the-ground radio links without the cost of additional infrastructure. Hence, whenever possible, neighboring client devices will use their direct connectivity capabilities, instead of infrastructure (cellular) links. Consequently, D2D connections are anticipated to become an effective solution that would unlock substantial gains in capacity and relieve congestion [9] on the way to 5G mobile networks. For mobile network operators, D2D connectivity is becoming vital to enable *traffic offloading* from the core network and to realize efficient support of social networking through device localization.

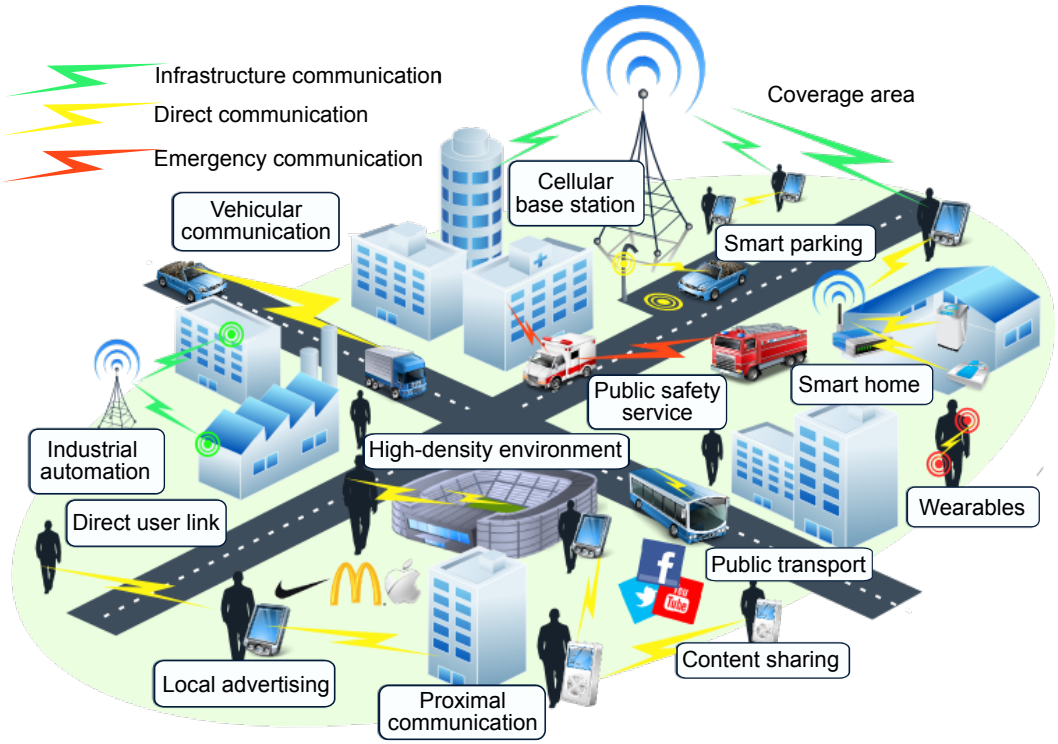


Figure 2.1 *Contemporary vision of proximal scenarios over D2D*

Fundamentally, proximity of user devices promises higher *data rates*, lower *transfer delays*, and better *power efficiency* [10]. More broadly, employing client devices within the integral network infrastructure is envisioned as the logical next step to improve spatial reuse towards the vision of 1000x capacity by the year 2020 in 5G systems. Consequently, over the past few years, D2D communications has received significant attention, both in industry and academia, due to the growing number of services and applications that could leverage the proximity benefits. The *prospective applications* of D2D connectivity in cellular networks are numerous (see Figure 2.1) and include, to name a few, local voice service (offloading calls between proximate users), multimedia content sharing, gaming, group multicast, context-aware applications, as well as public safety and national security.

Over the last decade, much research effort has been invested into the characterization of D2D connections as part of LTE cellular technology by 3GPP in *licensed bands*, where a license grants a network operator the right to use spectrum exclusively. Driven by a wealth of potential practical applications, the concept of D2D communications as an *underlay* to a cellular network has been developed by the seminal work in [11] and numerous subsequent papers. As in cognitive radio, D2D underlay is operating on the same resources as the cellular network and D2D users control their transmit power to suppress the resultant interference to the cellular users. Given its growing importance, the licensed-band D2D is becoming an attractive research area, where many fundamental questions still remain open. However, the corresponding *standardization* efforts are developing slowly, such that the respective products employing the D2D underlay may not be the first to meet the market.

Alternatively, *unlicensed* bands can be used freely, which gives opportunity to leverage D2D benefits almost immediately. While there already exists a plethora of unlicensed spectrum protocols to technically enable direct connectivity, there is neither centralized control of radio resources to manage QoS on D2D links nor is there any scalable device discovery solution [12]. Augmenting the current technology, the author envisions that devices be *continually associated* with the cellular network and use this connectivity to control their D2D connections in unlicensed bands. Therefore, in the near-term it is expected that the majority of gains will come from advanced *network-assisted* D2D architectures and protocols that would leverage the unlicensed spectrum.

2.1 Research background

Today, assisted proximal communications constitutes a *radical innovation* and thus becomes an exciting new area of investigation. Not surprisingly, researchers from different branches of science are flocking into this space, bringing an avalanche of recent publications on various aspects of direct connectivity. However, the true D2D technology is *very different* from the past concepts of delay- and disruption-tolerant networks, mobile ad hoc network (MANETs), as well as sensor and mesh networks in that it assumes a certain degree of cellular network assistance, coordination, or control of otherwise distributed proximal communication.

As discussed above, there are two distinct flavors of D2D technology: one currently available in unlicensed (e.g., ISM) bands, named *out-of-band*, and another standardized as a 4G add-on in licensed (e.g., cellular) spectrum, named *in-band*. Further, in-band D2D can be implemented as *underlay* (when D2D transmitters opportunistically access time-frequency resources occupied by cellular users) [13] or *overlay* (when cellular and D2D transmitters use orthogonal time-frequency resources) [14]. In what follows, the state-of-the-art along these lines is summarized.

2.1.1 Option A: in-band D2D in cellular networks

For more than 5 billion cellular clients registered today, network-assisted D2D communications is becoming a natural next step to achieve enhanced resource utilization as the traditional methods to improve the use of licensed spectrum approach their theoretical limits. Consequently, there has already been some coverage in literature on direct user connectivity with different levels of network involvement ranging from the minimal degrees of assistance (such as in Aura-net/FlashLinQ) [15] to the fully controlled solutions (such as in cellular underlay) [11]. The latter is naturally more challenging and generally requires interference control to enable simultaneous direct links [16].

For the D2D underlay/overlay to work, the network should employ proper admission and power control on D2D transmitters as well as allocate radio resource to them. As a result, D2D links may (i) reuse resources reserved for cellular use, (ii) use free resources not allocated for cellular use, or (iii) relay traffic through the infrastructure network avoiding direct transmissions. The choice between these alternatives is known as transmission *mode selection* [17] and has attracted many researchers

focusing on various optimization targets, from signal to interference plus noise ratio (SINR) and throughput to energy efficiency [18], data delay, fairness, and outage probability [19]. The general difference between existing works is in the considered numbers of communicating entities of each type (base stations, cellular and D2D users), emphasis on uplink (UL) or downlink (DL) connection and the resulting interference, orthogonal vs. non-orthogonal resource sharing, degree of available network assistance, and network/D2D duplexing mode.

In summary, the existing design and development efforts have been mostly based on static system-level simulations, whereas academic research has been focusing on simpler (and often even simplistic) system models to maintain analytical tractability. Some aspects of licensed spectrum D2D have indeed been evaluated, including the design of D2D-aware multiple-input and multiple-output (MIMO) schemes, application of network coding [20], successive interference cancellation, and even wireless video distribution over D2D [21]. As a result, 3GPP member companies are currently pushing for the standardization of D2D communications over licensed bands [22]. A major breakthrough was achieved in due course when 3GPP (in LTE Rel.-12) agreed on completing an assignment for D2D technology focusing primarily on proximity detection for public safety (known as 3GPP ProSe) [23]. As the result, D2D appears today as a 4G feature with very limited performance potential and much further work is required to having a D2D dimension *natively* supported in 5G (a.k.a. LTE-Direct). Meanwhile, as many important research challenges still remain open, the use of unlicensed spectrum for D2D is becoming an attractive immediate alternative.

2.1.2 Option B: leveraging out-of-band opportunities for D2D

In unlicensed spectrum, such as the industrial, scientific and medical (ISM) bands, no network may take advantage of exclusive spectrum usage. This results in uncontrolled wireless interference and lack of global synchronization, which requires a robust interference-proof solution. In the past, legacy Bluetooth and WiFi technologies have become increasingly widespread among users to organize wireless personal and local area networks respectively. Based on IEEE 802.11 standards, WiFi is currently a predominant choice for user device connectivity both with and without involving the infrastructure APs. Since it operates over shorter links and higher

frequencies, it achieves better levels of spatial reuse than 3GPP LTE. Hence, even poor WiFi link generally delivers higher data rate and energy efficiency than any today's cellular technology.

Importantly, the current WLAN technologies running on the unlicensed bands can be made to cause very little interference to LTE networks. But while this makes the use of WiFi an excellent choice for the network, this may not always be the case for the client. For example, WiFi connectivity lacks a fast and resource efficient way of notifying clients when/if they are in D2D range. Hence, if a user is searching for a particular peer who is out of range for a long period of time, it will suffer significant battery drain. Therefore, the QoS performance of uncoordinated short-range technologies may be limited by the lack of centralized management, which could otherwise facilitate peer discovery and medium access [24].

In other words, in conventional WLANs, the AP has no measures to control the resources used by ad hoc user connections, which contend for the same channel. This is where the LTE network can be of much help. If clients are continuously connected to the LTE network, it knows which cell(s) they are associated with, which tracking area(s) they are in, and their locations within a few meters (if location services are enabled). Therefore, the network can quickly and without significant overhead determine if/when clients are potentially within D2D range and inform them accordingly. Additionally, network assistance can help with mode selection [25], power control [26], and selecting transmission format (modulation and coding rates, MIMO transmission mode, etc.) [27]. Finally, with recent and emerging 802.11 protocols, such as WiFi-Direct (for infrastructure-less communications in ISM bands), 802.11ad (for data transmission in mmWave frequencies at extremely high rates), and 802.11ah (for machine-type communications in sub-1GHz spectrum at very low power), assisted out-of-band D2D connectivity holds a significant promise for further investigation.

2.2 Open challenges

In the remainder of this text, the author of this thesis outlines the currently open research challenges in the context of network-assisted proximal communication, solving which may eventually convert this promising technology into a *new commodity* for both network operators and end clients.

Challenge 1: proposing adequate D2D-aware scenarios

We expect that assisted proximal communications will become of high benefit in congested locations (e.g., office buildings, shopping malls, hotspots, airports, and public events) characterized by high daily densities of users, who may employ D2D and cellular links concurrently (see Figure 2.1) [28]. In existing research literature, however, the target D2D use cases are often selected arbitrarily and artificially, whereas standardization bodies have paid so far very limited attention to the *entire* palette of prospective D2D-inspired applications. In particular, past 3GPP Rel.-12 work has only been focused on public safety/national security domain [29] as well as on neighboring device/service discovery for commercial use. Hence, a fresh look is required to identify comprehensive available set of proximal scenarios.

Further, the envisioned D2D scenarios have to be distributed across the characteristic application categories, such as mobile proximity-based social networks; direct communications and offloading between smartphones, tablets, and laptops; e-commerce and location-based advertising; high-speed vehicular networks; machine-type communication; wearables; public safety (first responders), etc. Each such distinct area, in turn, has a number of alternative radio access technologies (RATs) that are (or will soon become) available in the respective market niche; and the research community might want to map each of these application areas onto the relevant subset of RATs. Finally, for every such area with its associated RATs, the major research questions have to be identified both from the mobile operator and the end user perspectives (which may have conflicting objectives). These questions could be formulated in terms of typical performance metrics (user data rate, energy efficiency, latency, network/area capacity, coverage probability, SINR distribution, etc.). In particular, special attention has to be paid to *environment dynamics* (traffic variability, user mobility, wireless channel fluctuations, etc.), which has not been adequately covered by the past literature.

Challenge 2: developing D2D-centric system architecture

Historically, existing wireless architectures had very limited coordination between different radio access network (RAN) types. For example, 3GPP (cellular) and WiFi (WLAN/IEEE 802.11) technologies had developed independently in the past, but recently the standards community has recognized the need for breaking this long-accepted paradigm. To this end, a range of RAT interworking methods has emerged,

from loose application-layer coupling and core network based coordination functions to the latest RAN-level integration options ratified in Rel.-12 LTE (and continued in Rel.-13). With tighter RAN-level coupling, the 3GPP and WLAN technologies may in principle interwork more dynamically. Hence, the author is confident that some forms of LTE-assisted WiFi D2D solutions may be useful in practical networks almost immediately [30], as contemporary handheld devices can already operate over D2D links in unlicensed bands. However, much additional work needs to be done along the lines of adding improved network assistance logic due to the rapid advent of (relatively) novel and emerging 802.11 technologies, such as WiFi-Direct, WiGig (802.11ad), and low-power WiFi (802.11ah).

Complementary to the above, the perspective of offering in-band D2D communications option (i.e., LTE-Direct) delivers even tighter synchronization between the devices, allows leveraging more advanced security procedures and transmission modes, and thus generally promises higher gains to both operators and clients (capacity and reuse factors, peak rates and latency, coverage extension, etc.) [31]. However, the respective progress in 3GPP is slow due to disjoint opinions and conflicting business strategies of the involved member companies. To this end, LTE Rel.-12 has only studied so far system requirements for D2D, as well as proposed simple architecture and physical-layer enhancements (see the corresponding 3GPP technical reports [32], [33], and [34]). This 3GPP work, while being a dramatic departure from infrastructure-only cellular communications paradigm, still requires significant effort to make LTE-Direct reality [35]. In particular, appropriate lightweight signaling and UL/DL duplexing frame structures have to be developed to integrate efficient support for direct-mode LTE [36]. This is especially important as LTE offers higher degrees of freedom in D2D mode selection, as well as potentially offers more fine-grained control over D2D pairing and subsequent communication.

Additional areas of research with respect to D2D system architecture include coupling direct-mode communications with (massive) MIMO schemes and other multi-antenna techniques [13], as well as harnessing mmWave frequencies for D2D connectivity with their associated unique challenge of highly directional transmissions [37]. More attention will be needed to learn the feasible levels of network assistance information (in terms of control protocol overheads), from user locations, channel knowledge, and network loading/interference factors, and up to expected user intentions (such as in emerging *user-in-the-loop* studies [38]). This, in turn, will require proper accounting for numerous real-world factors that are expected to influence the

performance of practical D2D deployments, such as actual traffic arrival patterns, user mobility behavior, air interface considerations, tight coupling between communicating devices and collocated access technologies, application service requirements, fine-grained channel degradation factors, etc. Ultimately, with the support from the cellular network, the author expects that D2D connectivity can be automated, and devices may enjoy D2D benefits anytime/anywhere without considerable human user involvement.

Challenge 3: designing efficient D2D operation mechanisms

In tight connection with proximity-aware network-assisted architecture work goes development of feasible D2D mechanisms at all stages of the process in question: device/service discovery, connection setup, and data communication. Improved device awareness alone, achieved with always-on proximal discovery, is expected to decisively augment the networks of today and eventually transform into the *digital sixth sense* [39]. Here, research is necessary on proposing improved discovery schemes [40], which would be superior to past similar location- and beacon-based methods (e.g., in IrDA, Bluetooth, as well as in conventional WiFi ad-hoc, WiFi-Direct, and cellular technologies). More generally, the forthcoming work includes redesigning the conventional network control functions for D2D [41], [42]: resource allocation, power control, interference coordination, seamless handover, etc., as well as proposing new schemes for e.g., mode selection and cooperative client relay [43]. To facilitate this study, our research group has recently built an advanced *system-level simulator* (SLS) based on up-to-date 3GPP LTE evaluation methodology and current IEEE 802.11 specifications. Today, neither free nor commercially-available simulation tools are readily applicable for developing D2D protocols as they are missing the necessary features, as well as lacking scalability to adequately capture the dependencies between the studied variables. By contrast, our SLS is a flexible tool targeted to support diverse deployment strategies, traffic models, channel characteristics, and wireless protocols [44].

The next natural step after the relevant D2D mechanisms have been delivered is to tailor them to the envisioned dense deployments [45], [28]. While there have been concerns that the quality of D2D connections may not be sufficient for higher user/infrastructure densities, our preliminary results indicate that the corresponding performance improvement is significant even with very simple forms of network assistance [46]. However, further work is necessary on D2D-aware radio resource

allocation and management (transmit power and neighbor/mode selection); interference coordination/cancellation and advanced receivers (where network manages the number and the selection of simultaneous D2D transmitters); efficient spectrum sharing (licensed vs. unlicensed); delay- and traffic-aware resource management [47]. Of particular interest are D2D-aided point-to-multipoint (multicasting) transmission schemes [48], [49] with appropriate device grouping (to optimize the respective choice of modulation and coding schemes) [50], [51]. Most importantly, a characteristic feature of ultra-dense networks is that occasionally they may be substantially underutilized (due to high variations in current loading), whereas conventional cellular networks are generally expected to soon meet their capacity limits. However, given the associated complexity, dynamic systems have not been studied as broadly as their static counterparts with a fixed set of active users. Consequently, our proposed future focus is on properly and explicitly accounting for said variability in user, traffic, and environment dynamics.

Finally, to conclude work on the D2D-specific control schemes, the promising selected mechanisms have to be converted into actual real-life 5G-grade direct protocols. This work includes careful design of appropriate signaling patterns and their respective optimization [52]. As an example, community needs to develop robust low-complexity procedures for D2D mode selection, which allow potential D2D partners to efficiently choose between silent, non-orthogonal sharing, orthogonal sharing, and cellular transmission regimes. While there is a challenge in that the resulting utility function for the general case may turn out to be overly-complex (or even intractable), the author of this thesis is confident that it would be possible to indicate feasible near-optimal (approximate) solutions with reasonable mathematical tractability [53]. These solutions will reveal the guiding design principles to deal with imperfect (non-ideal) control channels (e.g., capacity-limited, delayed, and with unreliable signaling). This, in turn, should allow for assessing the extent of minimal signaling overheads for efficient D2D operation, as well as effectively balance the developed intelligence between the users and the network.

Challenge 4: performance evaluation of D2D solutions

As it was presented previously, the development of adequate D2D operation mechanisms comes with its unique challenges, such as dual user mobility, low antenna heights, and high inter-link correlation. Therefore, a diversity of methods has to

be applied to assess the performance of perspective D2D-centric mechanisms. Today, known D2D performance evaluation works are based on (non-)cooperative, coalitional, and evolutionary game theory [54], [55] direct numerical analysis, graph theory [56], as well as simple forms of stochastic geometry [57] (that is, statistical modeling of spatial relationships) and utility maximization. However, these approaches are mostly restricted to (semi-)static D2D system topologies and/or may introduce prohibitive complexity for subsequent real-time implementation. In sharp contrast, the author proposes to adopt a range of random spatial models, where user locations are drawn from a particular realization of a random process, and then integrate them with appropriate flow-level dynamic frameworks [58]. Coupling such *topological randomness with system dynamics* introduces a fundamental difference in characterizing user signal power and interference, dynamic load modeling (e.g., streaming traffic vs. bursty files), handovers, etc. The group has already made progress along these lines [30] and possess preliminary results that demonstrate that the *locations* of the network clients relative to each other highly impact the resulting system performance [46].

Capitalizing on the methods proposed for D2D analysis, the research community would need to develop further understanding behind the anticipated performance of proximal communications on the system level, including coverage and capacity projections (coverage probability, number of served users, their throughput, etc.), as well as characterize spectral and energy efficiencies across the entire D2D deployment, its operational latency and reliability. In the absence of prior information about user locations, the author began with the simplest statistical tool to model user placement with a uniform distribution, which in the two-dimensional plane corresponds to a homogeneous (stationary) Poisson Point Process (PPP). This model is surprisingly tractable and provides a reasonable first-order understanding of random deployments [59], which then needs to be coupled with flow dynamics to achieve better load balancing between e.g., voice vs. data. Then, the models in question could be extended to more realistic, but also significantly more complex point processes, such as binomial process spawning a fixed number of users in a given area and Poisson cluster process allowing transmitters to group in certain locations. Eventually, it should become possible to attack the most challenging hard core point process which is a thinning of the PPP such that the users have a guaranteed minimum separation (due to e.g., excluding carrier-sensing range).

To comprehensively conclude on the performance promise of proximal systems, researchers need to build a general mathematical framework for assisted D2D connectivity featuring the analysis of achievable area capacity regions and gains, advanced interference mitigation approaches for simultaneous D2D pairs, benefits of single- vs. multi-hop communication [60], and other new fundamental knowledge and methods. More generally, studying the *capacity* of D2D-capable wireless networks remains an open problem in the field of information theory, and in order to shed light on it our need is to explicitly capture new interference situations and hence the achievable data rates. This is indeed a very ambitious task as it requires advanced mathematical knowledge to interconnect and apply techniques and methods coming from the area of point processes, probability theory, queuing theory, and percolation theory, as well as modern engineering insights [61]. Another challenge is to account for high mobility of potential D2D users, when direct connectivity graphs become extremely unstable [56]. In addition, we also need to understand the added value of emerging new techniques for D2D, such as energy harvesting (especially for machine-type devices), cognitive radio improvements, and interference randomization via time/frequency hopping.

Challenge 5: leveraging available D2D benefits for operators

Utilizing the solutions to the above challenges, further work could be targeted at a thorough characterization of dynamic *cellular traffic offloading* onto the direct links to relieve congestion in pre-5G deployments [62]. Many believe that this form of offloading will be preferred by mobile network operators at around 2020 due to reduced operational and capital investments associated with D2D operation. The author, proposes to address efficient data dissemination methods over D2D in coexistence with alternative forms of offloading (WLAN-based, small cells, ultra-dense heterogeneous networks, additional spectrum with LSA, and mmWave access) [63]. Naturally, depending on the client mobility patterns, some services are better suitable for proximity-based network offloading than the others. For example, if D2D partners are non-stationary, the quality of the link may change dramatically over short periods of time, thus making it difficult to guarantee service. In these cases, the best candidates for proximal offloading are delay-tolerant services, i.e. those that can be queued until the D2D link recovers or for which the data session can be moved to the infrastructure network (e.g., video-on-demand or file transfers). However, if both clients are (semi-)stationary, many other services, such as cooperative stream-

ing and social gaming, can be offloaded onto D2D links with good results. Further, the author envisions massive performance gains for mobile network operators, that will come from *inter-cell load coordination* for non-uniform user traffic (i.e., 1% of clients generating around 10% of traffic [64]) in flow, space, and time [65]. Indeed, it is well known that wireless capacity cannot generally be transferred (stored) in *time* as well as it cannot be transferred (moved around) in *space*. However, several alternative opportunistic approaches may be used to work around these fundamental restrictions and arrive at more uniform network loading and ubiquitous space-time service with minimal risks to the conventional network behaviour, which is much desired by the operators today.

To aid early adoption of D2D communications by mobile network operators, the appropriate incentive mechanisms would also need to be in place. These should include novel D2D-aware pricing and billing schemes, which may encourage D2D-based cooperation across the network. In tight connection with such schemes goes user categorization into service classes (platinum, gold, silver, bronze, etc.) with respective sets of guaranteed and best-effort services. Not only should this impact the choice of network-wide resource allocation criteria, but also influence the user admission procedures onto cellular vs. D2D tiers. Naturally, the densest packing of D2D pairs should be catered for (a.k.a., maximal matching), such that the predefined levels of quality of service/experience could be maintained (e.g., minimum bitrate, latency, availability), mindful of the time required to perform such packing. Our research group envisions that the field of integral geometry embodies applicable methods, such as the notion of kinematic density, which will enable us to understand the best available packing schemes of D2D pairs, when direct-mode communications is employed. Ultimately, research work along the lines of this challenge should help identify existing and offer new incentivized services over D2D together with appropriate monetization opportunities for network and technology operators, as well as for the over-the-top providers, to eventually enrich the entire 5G service ecosystem [66].

Challenge 6: leveraging available D2D benefits for clients

Complementary to the previous challenge, a look at the D2D solutions benefiting network clients is required. Here, *proximity-aware user-specific algorithms and strategies* are in prompt need, which are able to efficiently leverage direct connectivity in emerging 5G networks, thus resulting in novel practices for end users. An important challenge for individual users, as well as for connected mobile clouds,

remains in the insufficient degrees of availability of user-desired content. Here, D2D systems can be of much help by caching the most popular content locally in the neighboring user devices [67], thus dramatically improving content availability and bringing the service *closer* to the end user. Another interesting development is to explicitly account for the end-user *traffic activity* [68] and shape it, which has recently been named user-in-the-loop [38]. Indeed, as human users tend to exploit more and more services and applications on their mobile devices, they are often left frustrated when these do not work anytime/anywhere. Network operators are thus forced to invest astonishing amounts (of up to $50 billion per year) into improving their network infrastructure, but the seminal work in [38] proposes an attractive alternative by actually *impacting* user-generated traffic, which could be investigated further for D2D systems.

Finally, a set of security-related challenges is arising, as user adoption is inherently intertwined with the sense of security, privacy, and trust towards a particular service or application. Hence, the community needs to address the coexistence of closed vs. open access groups [69], especially in the cases of partial/no network coverage [70] (edge of a cell, network failure, malicious attack, etc.), and offer provable security and privacy mechanisms for such novel scenarios.

3. SECURING INTERMITTENT CONNECTIVITY

In today's cellular networks, the central control infrastructure that orchestrates the associated wireless devices is deemed always available [71]. Consequently, given its reliable and ubiquitous presence, cellular network is typically assumed to serve as a *trusted authority* for security purposes. In proximity-based D2D communications 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 thus be handled over the PKI [72].

3.1 Cellular networks of today

For wireless architectures not relying on pre-existing network infrastructure [73, 74], communications and security functions are distributed across users. If simultaneous use of more than one radio interface is allowed, a variety of new attacks [75, 76] become possible, which advocates the use of PKI whenever available.

The key requirements for hybrid systems without permanent centralized management can be identified as follows [77]: a reliable connection establishment control algorithm; an adaptive mechanism for rapid response to network topology changes or node failures; a multi-hop communications possibility; and an **algorithm enabling continuous secure connectivity** even when the cellular base station is not accessible. This important topic is elaborated upon in what follows.

Currently, the research area of secure proximity-based connectivity is being established from the optimal resources allocation [78], key redistribution [79], and physical security [80] perspectives. Importantly, the suggested protocol to allow secured direct interconnection in combined cellular/WiFi networks would require a strong response from industry. This fact is due to the complexity of its implementation and standardization processes.

Before proceeding with the associated background, the author of this work discusses the main underlying terms and definitions. First, a security protocol is assumed to be composed of distinct *blocks*, which in essence constitute various cryptographic primitives constructed by the protocol developer or reused from the past research. Each of these primitives solves a certain specific security issue. Some fundamental primitives and their associated descriptions are the following:

- Confidentiality (Encryption) – only authorized users have access to the data transmitted over a wireless network.
- Integrity (Hash functions) – only authorized users can alter the transmitted data.
- Accessibility (Keys, Passphrases) – only authorized users can access the data in a timely fashion within operational constraints.

As a result, relevant primitives are combined in order to construct a required protocol that would solve a certain target task. In particular, important research questions to address when developing the protocol are: *What to combine? How to connect? In which order?*

3.2 Secure connectivity for unfamiliar devices

This section concentrates on the key security challenges from the point of view of establishing secure connectivity between *unfamiliar* proximal devices. Even though our problem formulation is novel and shaped by the emerging network-assisted D2D technology, the topic itself has much prior background captured e.g., in [81, 82], and [83]. For instance, the well-known Diffie-Hellman key exchange algorithm [84] maintains the zero-knowledge property on each side of communication, but requires a secure channel in-between the communicating parties for its successful operation. Taking into account the more recent developments, PKI is employed as a *trusted authority* (i.e., a certificate provider) to distribute public keys and by this means allowing the communications for end-devices [72]. A simplified PKI scheme is depicted in Figure 3.1.

Alternatively, if the network in question does not feature a centralized control unit, a *Pair-Wise Key* (PWK) could be utilized [85]. Importantly, while using this method

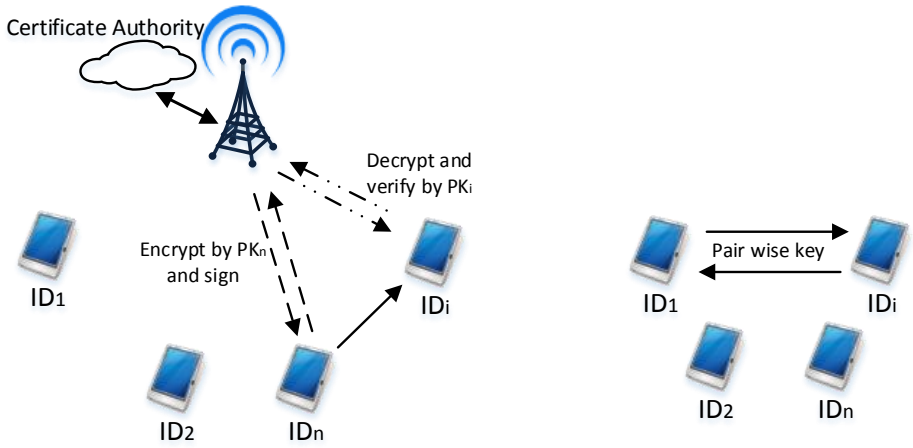


Figure 3.1 *Secure data transmission with and without the PKI*

the communicating devices would not be able to obtain any information about their pair devices except for their identity. Hence, one would need to use *ID-based cryptography* [86] and verify the device's signature – a public key based on a specific ID. However, a personal secret key is then required for decryption. The respective service may be provided with the use of a *Private Key Generator* (PKG), which could be employed only in the case of its availability in the system.

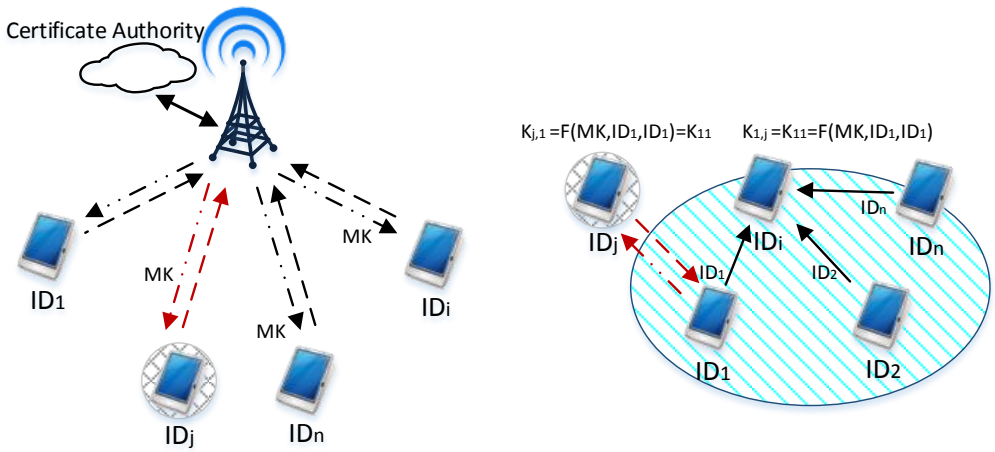


Figure 3.2 *Keys (pair-wise) redistribution and new user arrival case*

Additionally, if a PKG becomes temporarily unreachable, a set of users connected to the PKG prior to when the connection became unavailable could group together and form a (or use an existing) *Master Key* (MK) [87], [88]. Accordingly, a new device

could receive access to the network as it is shown in Figure 3.2. A new PWK could be generated as a function of the MK and a set of IDs ($F_{i,j} = F(MK, ID_i, ID_j)$).

Interestingly, in sensor networks the devices conventionally remove the MK after the key pair generation has been completed [89]. Such course of operation is taken mainly due to the static system topology of most sensor networks. Along these lines, in our D2D architecture we reuse this approach in order to allow for the new devices to join the network continuously, even if the cellular network connection becomes unreachable. Additionally, the MK would be regenerated anew in case when the base station connection is re-established.

Noteworthy, the devices may also store a PWK with themselves $F_{i,i}$. This is done mainly for the case when a new user enters their proximity, that is, when the target device is connected to the cellular network and it requests a MK directly from the network coordinator to obtain a new key and connect to the neighboring device $K_{1,j} = K_{1,1} = F(MK, ID_1, ID_1)$.

Another important issue in proximity-based networks is the question of *trust*. In this thesis, the author considers a solution based on *Pretty Good Privacy* (PGP) trust scheme developed by Phil Zimmermann [90]. Accordingly, the trust level can be input as a numeral from zero to one and would then be obtained as a sum of the trust multiplications for the already known users $t = w_{01}w_{11} + w_{02}w_{12}$, as it is demonstrated in Figure 3.3. Hence, if the trust level is equal or greater than 1, one can assume that the user is trusted; otherwise, the connection to this user would be discarded. In addition, one may build a tree of trust for the target network.

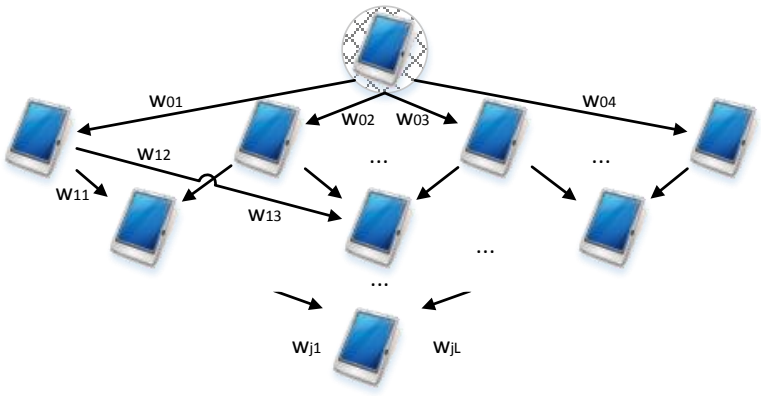


Figure 3.3 *Trust policy based on PGP scheme*

The second part of our discussion concerns classical issues related to ad-hoc networks [91], that is, proximity-based device arrival/departure when no connection to the centralized infrastructure is available. Importantly, this scenario brings along additional challenges, such as key distribution for device association. The latter can be solved by a *Broadcast Encryption Protocol* [92], which implies that there exists a number of user key sets $K = K_1, K_2, ..., K_n$, where $|K_i| \geqslant 1, \cup K_i = K, |K_i \cap K_j| \geqslant 1$. In turn, for the key construction one may use *Cover Free Families* (CFF) – a specialized system of sets having the alphabet of elements X and a set of subsets (blocks) $F(X)$. An example of CFF is shown in Figure 3.4. Correspondingly, a system can be defined as a CFF, if for any block $B_0 \in B$ and any other r blocks $A_1; ...; A_n \in B$, one can calculate $B_0 = \bigcup_{j=1}^{r} A_j, =$ where $|X| = T$ is the alphabet size, $|B_0| = N$ is the number of blocks, r is the number of blocks, which do not cover any other block, and n is the block length.

As different users should have a possibility to obtain their key, there may appear a situation when a small set of users can produce the key with less inter-operation. Hence, the respective attack may be conducted by a certain group of devices. On the other hand, by using this approach one can guarantee that if the number of devices is less or equal than the minimum number of needed devices for the key reconstruction I, this group would not cover a key of any other device.

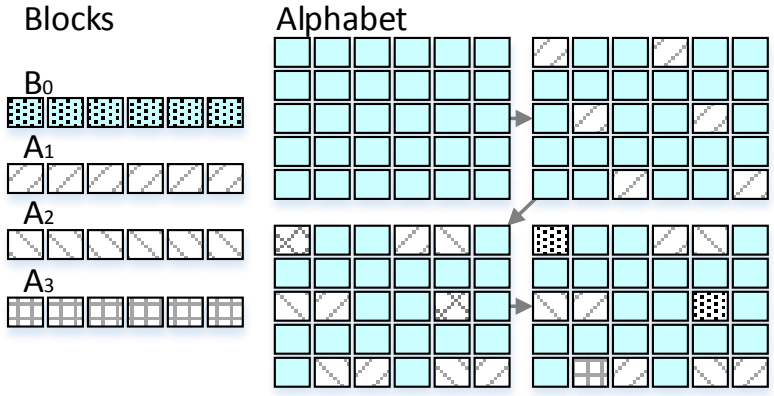


Figure 3.4 *Cover-free family $r = 2$, $n = 6$, and $T = 30$*

In summary, for our problem at hand one may employ sharing schemes based on well-known solutions, such as: Chinese remainder theorem [93]; Lagrange polynomial interpolation [94]; Error-correcting codes (Reed-Solomon codes) [95]. Providing continuous secure connectivity with the above solution should become a significant

improvement in next-generation D2D systems. Here, the Lagrange polynomial mechanism may be preferred due to its relative computational simplicity, which is one of the crucial factors for today's mobile devices. A classical formulation assumes that every communicating device (representing its user) is fairly equal and has the same weight of its *vote* (or share) in the overall trust tree. However, a situation may appear when one would like to vary weights and focus the discussed solution on the trust enforcement in more complex systems. Therefore, one would need to sign the data before transmitting it and employ the secret sharing schemes, which distribute the *key shares* between the devices. The following list is surveying the currently available *democratic* solutions [96]:

- (1,n) scheme – any individual device share can recover the secret key (shown in Figure 3.5a).
- (n,n) scheme – only all n shares from n devices can recover the secret key (shown in Figure 3.5b).
- (k,n) scheme – any k of n shares can recover the secret key. If the number of shares is less than k, then the key may not be recovered (shown in Figure 3.5c). This mechanism is chosen to be used in our implementation discussed below.
- weighted (k,n) scheme – participants with the weight sum of equal to or more than k can recover the secret key. The weighs may vary based on the level of trust (shown in Figure 3.5d).

In addition to the above, it is important to take into account the well-known *dictatorship* solutions [97]. The main difference between these and the previously discussed democratic approaches is in that one or more "significant" devices should participate in the key recovery process, and in case none has participated the key should not be recovered. More specifically, we assume that the *secret* is a codeword a of the Web Host Manager code [98], an *encrypted secret* is $b = a + e$, and the *shares* are the values and positions of possible fixed errors. Hence, the secret reconstruction process is essentially error correction at known positions of b. If the sum weight of uncorrected errors is less than the threshold value t, then the secret can be reconstructed by the decoding procedure.

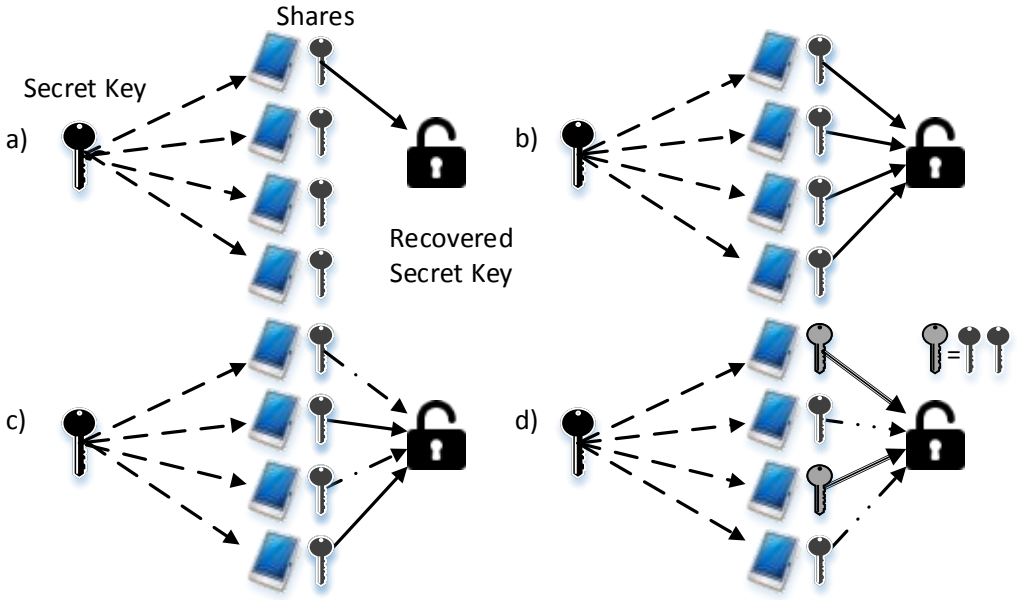


Figure 3.5 *Examples of secret sharing schemes*

Further, the proximity-based D2D system may be improved by employing the McEliece scheme for error-correcting codes [99]. Here, the secret keys for the security classes are chosen by means of using the embedded codes. Hence, each device has its own private key and no additional information on this specific device is sent in the encrypted message. Noteworthy, there is an opportunity to exchange messages on all levels of hierarchy, that is, in-between the classes.

In summary, the considered D2D system operation may look similar to that of ad hoc networks, but it also has one key difference – in a D2D scenario all the communicating devices are (have been) associated with the cellular base station, at least for some time, which would be sufficient to distribute the initial amount of 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.

4. INFORMATION SECURITY MECHANISM

Many contemporary mobile devices have several available short-range radio interfaces (WiFi, BLE, etc.) as well as employ cellular connection (e.g., 3GPP LTE) for most of their operation time. Hence, regular functioning of network-assisted D2D communications assumes that the cellular base station controls direct transmissions between devices (e.g., over WiFi-Direct) in all respects, including security, through the active cellular connection. However, if this cellular link is (temporarily) unavailable, secure communications may be disrupted and admission/exclusion of users to/from secure communications groups is not possible any longer. Taking advantage of the above background, below the author proposes a *novel mechanism* to extend the secure D2D operation for the cases of intermittent cellular connectivity.

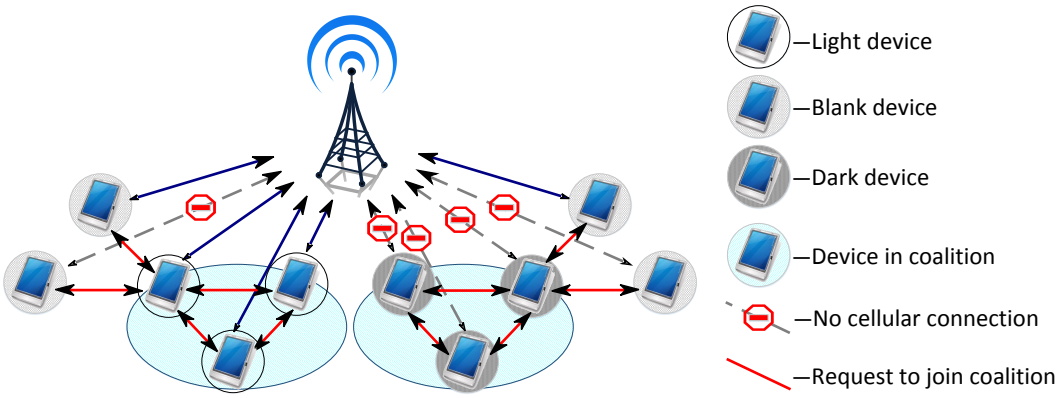


Figure 4.1 *Example scenario with unreliable cellular connectivity*

The target scenario (see Figure 4.1) considers all of the involved devices to be multi-radio terminals (at least with LTE and WiFi interfaces) that initially have been connected to the cellular network, which acts as their trusted authority for the purposes of the certificate distribution. Further, it is assumed that all of the devices under consideration participate in assisted offloading of their cellular data flows onto WiFi-Direct sessions [64], thus the cellular link is only taken into consideration for

transferring the signaling information. This link is employed by the D2D users in proximity to communicate with the PKI functions and establish a *coalition*, that is, a logical group of securely-commutating devices.

In this work, the author argues that whenever the reliable cellular link becomes unavailable for some of the devices in a coalition, additional measures are necessary to continue secure operation (communication, new user admission, user exclusion, etc.). Therefore, the author proposes the following classification to conveniently differentiate between the various types of users (see Figure 4.1) from the point of view of this research:

- *"Light"* device that has a reliable cellular connection active;
- *"Dark"* device that currently does not have a reliable cellular connection, but used to have such form of connectivity in the past;
- *"Blank"* (unknown) device that wishes to join the secure coalition. Importantly, such device may not have had access to the cellular network (and its respective trusted authority) previously.

To this end, the author of this thesis further specifies the following functions of the target algorithm to enable secure D2D communications in case of unreliable cellular connectivity.

Join coalition In case when a device wishes to join a secure coalition, the latter may be done in two alternative ways, depending on the availability of the cellular connection. If it is available, all the respective functions would be managed by the trusted authority residing in the cellular operator's network. The existing signaling mechanisms would then process the device's request straightforwardly by allowing to obtain its own certificate signed by the coalition owner. Alternatively, in case of unreliable cellular link, the device would send its request to any of its proximate users in the target coalition, which would then utilize the developed cryptographic methods, such as new user secret generation, certificates redistribution, etc. The coalition acceptance decision for this requesting device is made collectively, i.e., when k out of N devices in a coalition grant access to the new user based on their *shares*. Noteworthy, after the cellular connection is re-established for the new user, its inclusion into the coalition would be transparent for the trusted authority, as its secret is kept unchanged.

Leave coalition At some point, a device may decide to leave its current coalition due to mobility (i.e., leaving proximity) or other factors. This work considers the case of device exclusion and again different procedures could be applied. On the one hand, if the device in question has a reliable connection to the cellular network, which knows about its geographic position change, an automated decision can be made and user certificates for this specific coalition would be revoked. On the other hand, if there is no reliable cellular connectivity for this device, the decision should be made employing our proposed weight-based mechanism.

Coalition initialization Another important challenge is the initial device grouping. Again, for a system with persistent cellular connection, the devices can rely on the solutions from past literature. However, if not all of the devices involved into direct communications have a reliable cellular link, we need to reconsider the trust and privacy policies along the lines of this proposal.

Coalition recovery As defined before, the coalition is a logical group of devices with their own set of certificates. Hence, the dedicated measures are required to control the overall system stability in case when a coalition member misbehaves or comes into proximity of another already established coalition. Of particular interest are the situations when not all of the devices in the coalition have a reliable cellular connection available. In these situations, a modification of Diffie-Hellman key exchange procedure may be employed, followed by the challenge of introducing such a "remote" coalition to the cellular trusted authority.

Having described the most essential functions of the proposed algorithm on the general level, we can now proceed with discussing its actual implementation.

4.1 Securing direct communications

Although the D2D system operation may, at first glance, appear similar to that of ad hoc networks, there is one key difference allowing to relax 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. Hence, classical decentralized security-centric solutions (for e.g., sensor networks) may be significantly augmented in the D2D scenarios by utilizing the possibility to (periodically) access the trusted cellular infrastructure.

When designing our security solution, the author assumes 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 Figure 4.2 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.

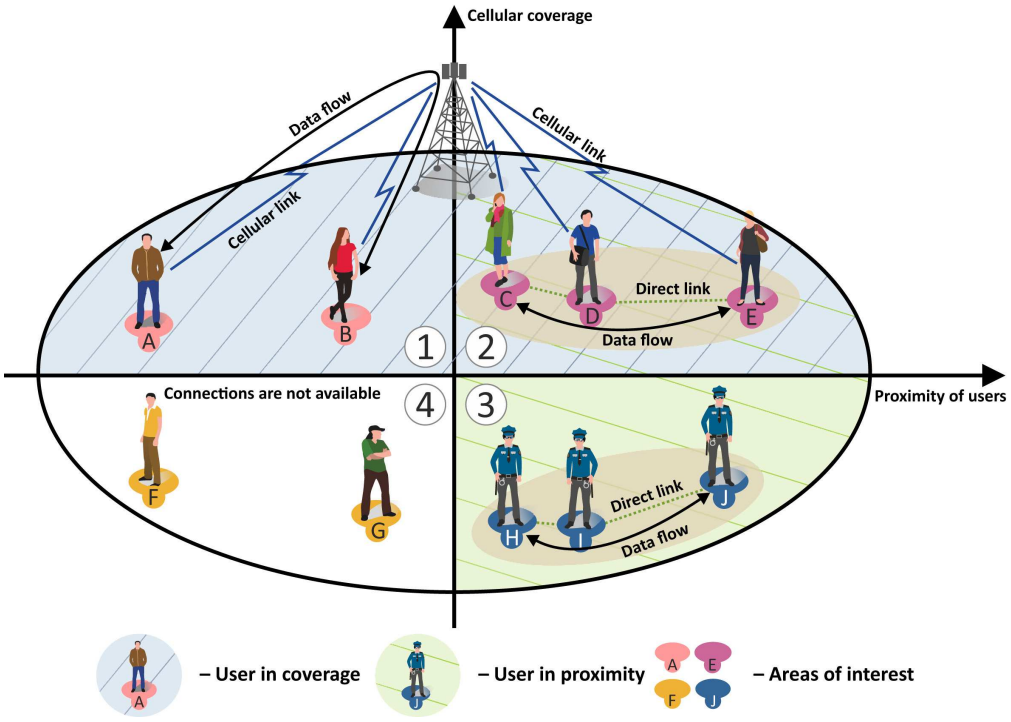


Figure 4.2 *Available D2D system operation modes*

- *Case 1.* Here, the grouped together users A and B have already established their own secure group (i.e., *coalition*) based on their area of interest and 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, the author focuses 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 and 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 when 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 the proposed security protocol, it is assumed 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. This thesis classifies 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 the one wishing to join the coalition for the first time. In what follows, the author addresses the crucial procedures of coalition initialization and formation.

As suggested in the previous Chapter, a remote server in the network core or in the Internet operates as a trusted authority for the application users, i.e., the server

certificate PK_{TR}, N_{TR} is distributed along with the application though the repository as it is shown in Figure 4.3. Importantly, all the cellular base stations of the operator are connected to this server and may concurrently distribute the coalition certificates signed by the TA, that is, PK_c and SK_c. Alternatively, those certificates may be distributed directly via a cellular link from the TA.

Recalling the above, all the communicating devices have a pre-generated set of parameters: ID_i is a unique identifier assigned for the i^{th} device using a particular application and PK_{TR} is a trusted authority certificate in order to verify the validity of the coalition and other devices (users). Additionally, each of the D2D partners would obtain a PK_c in relation to a specific coalition and then generate the PK_i – its own public key, the secret key SK_i, and a certificate share $cert_i$ signed by the SK_c. Here, the author defines $cert_i$ as a primitive for the Shamir's secret sharing scheme, i.e., the RSA-based algorithm for the sake of simplicity. These parameters are, in turn, required for the appropriate protocol operation in our target D2D scenario.

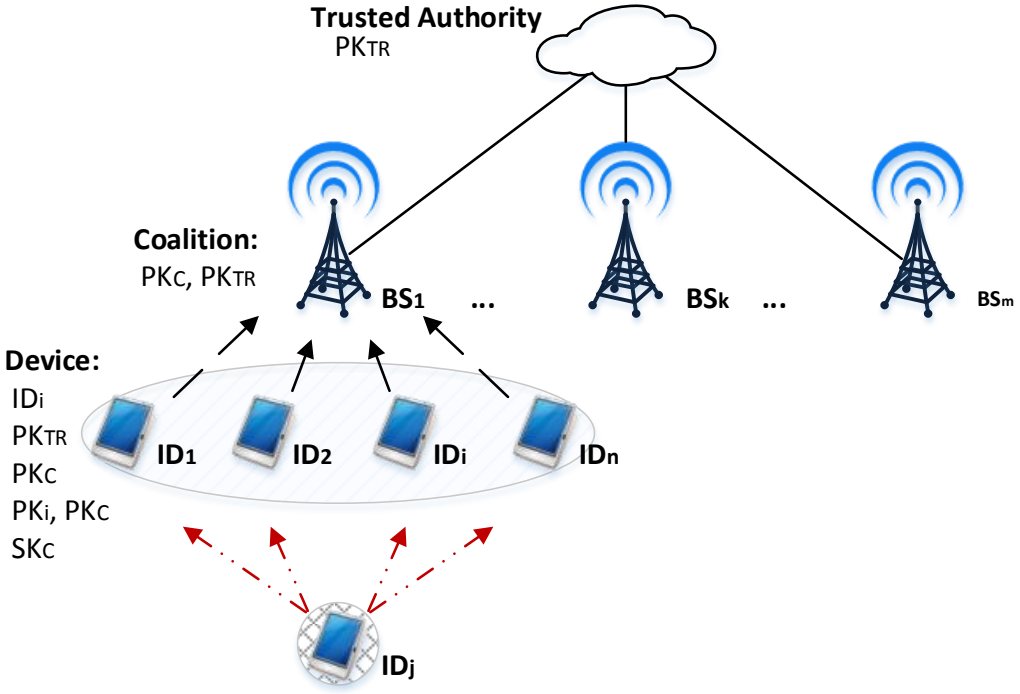


Figure 4.3 *Network topology from the coalition's point of view*

Initially, it is required that all of the devices have a reliable cellular connection to the TA and thus the author of this work outlines the case for a new *blank* device to **join a coalition** of *light* devices. Importantly, the actual cellular connection status of

the joining device is not important for the proposed protocol operation. However, as the existence of two protocol stacks for different connectivity states is assumed (ad hoc for WiFi and infrastructure for LTE), there is a need to consider these in details. For the infrastructure case, certificate distribution is a well-known PKI task, i.e., a new device is requesting the base station directly to join the target coalition. The BS then has to redistribute the new certificates for all the communicating devices belonging to this coalition.

On the other hand, the cellular connection may be unavailable for (some of) the devices in the coalition when a new device requests to join it – this is the case when a *blank* device is joining the *dark* group. Accordingly, the joining device is initialized by generating the PK_i and SK_i. Based on the fact that none of the devices have their connection to the TA at the moment, the author relies on the coalition itself when admitting the additional device. This, in turn, requires a *preset* parameter included into the PK_c certificate, which is a threshold value of k characterizing the number of devices in the target coalition that have a right to allow the new device to join it. This threshold value is chosen at the stage of coalition initialization and may vary based on the number of devices n and/or other factors; thereby a new certificate would be obtained for the joining user that is indistinguishable for the base station.

From the mathematical point of view, this procedure may be implemented at the base station side as follows

$$\begin{aligned} f(x) &= a_{k-1}x^{k-1} + a_{k-2}x^{k-2} + ... + a_1x + SK_c, \\ f(0) &= SK_c, \end{aligned} \tag{4.1}$$

where a_i is the generated polynomial indexes, k is the preset threshold value, x is the unique device identifier ID_i, and SK_c is the coalition secret generated for the secure group. Again, for the infrastructure case, the procedure in question is fairly straightforward, but in the distributed scenario the grouped devices should construct a secret for the new user without the cellular connectivity and not disclosing this secret to anyone. For both of the above cases, the certificate component for the j^{th} device is calculated as

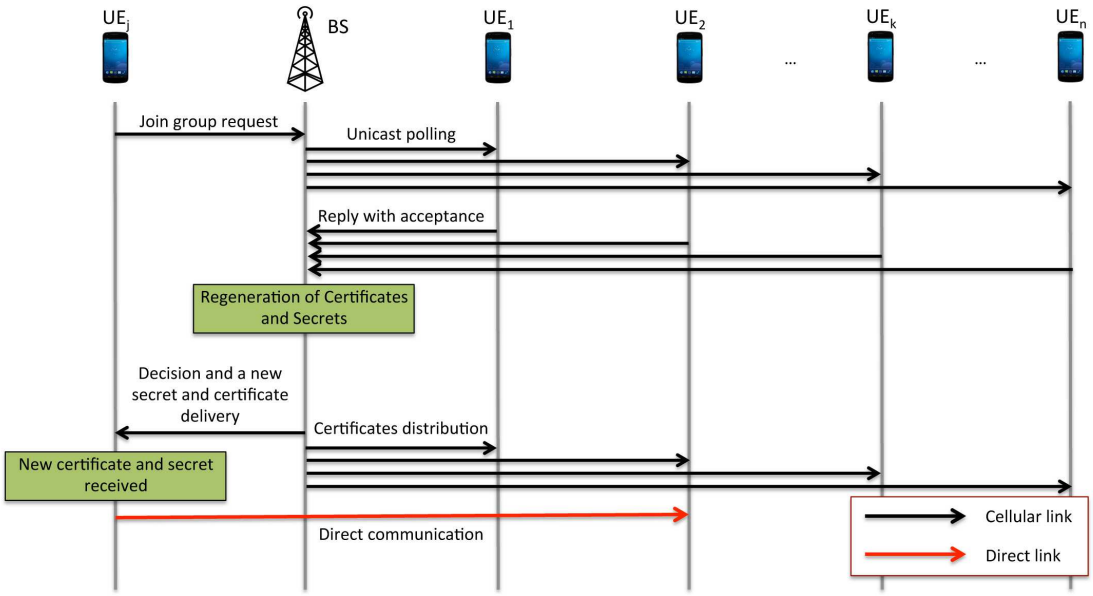


Figure 4.4 *Protocol operation in case of reliable cellular connectivity*

$$cert_j = \overline{PK_j}^{f(0)} mod\ N_c, \tag{4.2}$$

where $\overline{PK_j}$ is generated by the device with additional salt s_j: $(PK_j + s_j)$, $f(0)$ is the coalition secret obtained with equation 4.1, which can be either recovered or used at the base station itself, and N_c is generated at the coalition initialization stage as well.

In the case when the coalition is losing the cellular connection (that is, turns *dark*) and a new j^{th} device is willing to join it, we should consider a more complicated distributed protocol operation, as it is shown in Figure 4.5. If at least k devices have agreed to let the new device in, then a Lagrange polynomial sequence [100] is employed by allowing one to obtain the value of the function at any point $f(ID_j)$. Using the equation 4.1 in the Shamir's secret sharing scheme, $f(ID_i)$ could be obtained as

$$f(ID_j) = \sum_{i=0}^{k} f(ID_i) l_i(ID_j), \tag{4.3}$$

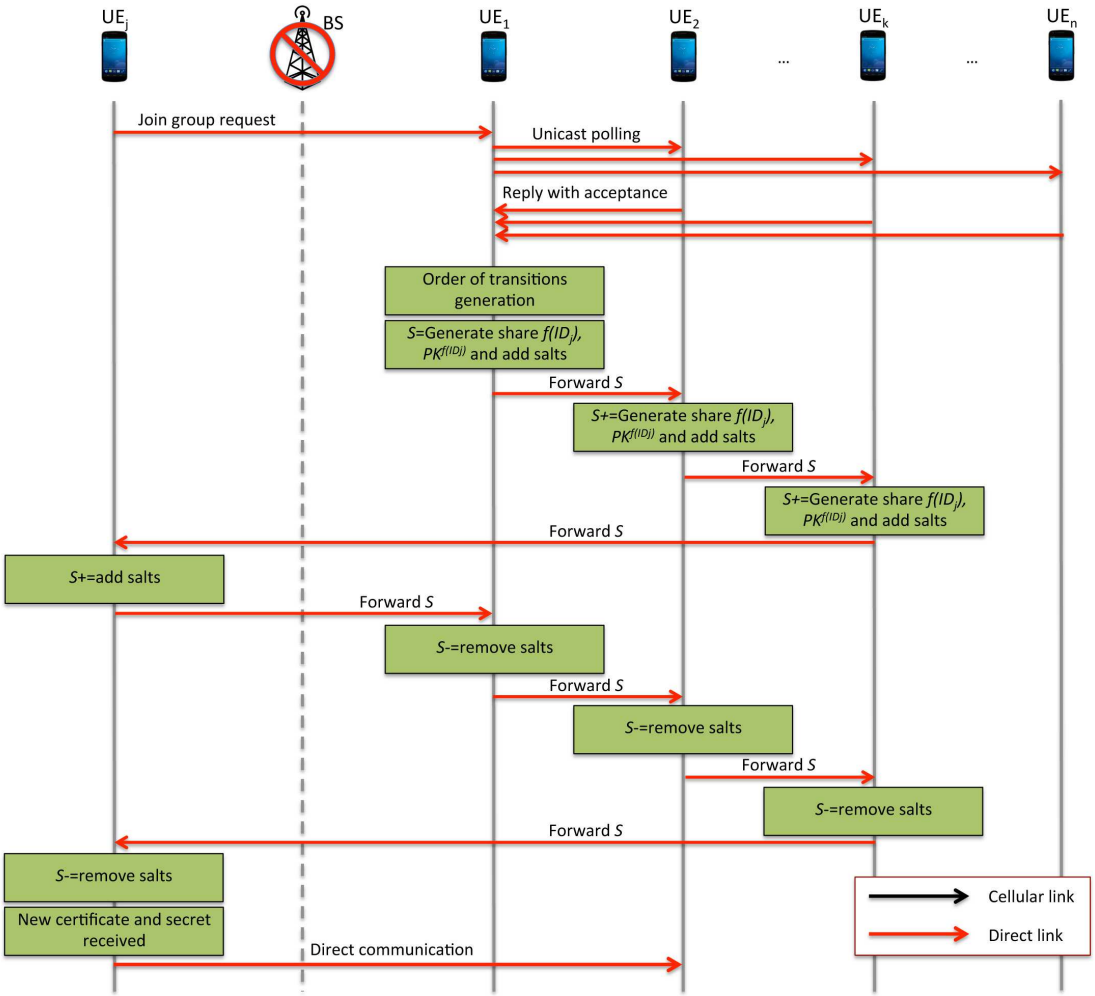


Figure 4.5 *Protocol operation in case of unreliable cellular connectivity*

where k is the threshold value and l_i is obtained as

$$l_i(ID_j) = \prod_{\substack{0 \leq m \leq k \\ m \neq i}} \frac{ID_j - ID_m}{ID_i - ID_m} \, mod \, \varphi(N_c), \tag{4.4}$$

where devices obtain their shares by utilizing the standard Shamir's mechanism and φ is the Euler's formula, given that the computations are done in the modular arithmetic.

Importantly, parts of the equation 4.3 are calculated individually at the device side and it is not allowed to distribute/share these between the devices due to the fact that their own secrets are involved into the generation process, whereas the IDs are publicly available. The required protocol steps are given in Figure 4.5 and detailed as follows:

1. The joining j^{th} device is sending its request along with its ID_j to the first one of the devices that has agreed to admit the former into the coalition.
2. The device with ID_1 is calculating its part based on equation 4.3 and adds its salt to the result $\overline{f(ID_i)} = f(ID_i)l_i(ID_j) + s_i$, where s_i is stored in memory.
3. The first device is then sending its result to the next device.
4. Steps 2 and 3 are repeated for all of the k devices.
5. The k^{th} device is sending the final sum back to the joining j^{th} device, which then adds its salt s_j to the equation and sends it to the first device.
6. All of the k devices are excluding their salts one by one similarly to the salt adding procedure.
7. The j^{th} device is excluding its salt an by doing so obtains its needed secret $f(ID_j)$.

The following protocol step is to generate the certificate for the newly joining device. For the infrastructure case, it can be obtained by using the equation 4.2. In the distributed scenario, k devices can recover $f(0)$ by grouping together as

$$cert_j = PK_j^{SK_c} mod\, N_c = PK_j^{f(0)} mod\, N_c = \prod_{i=0}^{k} PK_i^{f(ID_i)} mod\, N_c, \qquad (4.5)$$

which should be calculated similarly to equation 4.1.

Further, there is a need to consider the situation when the device is **leaving its coalition** based on e.g., weak proximity. The respective decision may be made by the group or by the device itself. For the infrastructure case this action is nearly trivial, whereas for the distributed scenario the respective operation has been shown

previously. Importantly, the main challenge here is still rooted into the key re-generation process for the updated *dark* group when excluding the j^{th} device. Note that SK_c and PK_c should be kept unchanged while new keys are re-generated and re-distributed for the updated coalition. Here, it is essential to follow the rule: the devices reaching cellular coverage again should be verified for their coalition membership. In addition, as it has been mentioned before, SK_c must not be recovered by any of the communicating devices. Therefore, $f(ID_i)$ should be reevaluated while keeping the original SK_c, which can be calculated as

$$f(ID_i) = b_{k-1}x^{k-1} + ... + b_1x + SK_c, \tag{4.6}$$

where indexes $b_{k-1} = a_{k-1} + \Delta_{k-1}$ and Δ_i may be generated by one of the trusted devices in the coalition. Accordingly, new keys could be derived for each user in the new group and then re-generate the certificates for all except the rogue device

$$f(ID_i) = a_{k-1}x^{k-1} + \Delta_{k-1}x^{k-1} + ... + a_1x + \Delta_1x + SK_c = f(0) + \Delta_{k-1}x^{k-1} + ... + \Delta_1x. \tag{4.7}$$

Finally, it should be noted that if a new device (or a group of the devices) acquires its new key, then it is not required to specify the source – it can be obtained directly from other coalition and does not depend on the connectivity state. However, this solution potentially accentuates an important security challenge: if there are k malicious users, they can form their own group and exclude other devices one by one. The author, however, considers this situation unlikely and leaves its consideration to the future research activity. In summary, the work arrives at a point of the complete mathematical model for the proposed D2D-centric information security protocol, and hence the discussion can now proceed with outlining the potential scenarios for secure proximity-based communications enabled by it.

5. PERFOMANCE EVALUATION

To evaluate the performance of the proposed information security approach summarized in Chapter 4, a simulation-based campaign has been conducted using the WINTERsim tool available at [44]. 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 Figure 5.1. 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 [101], [102], and [103]. The parameter α allows to adjust the form of the step-size distributions.

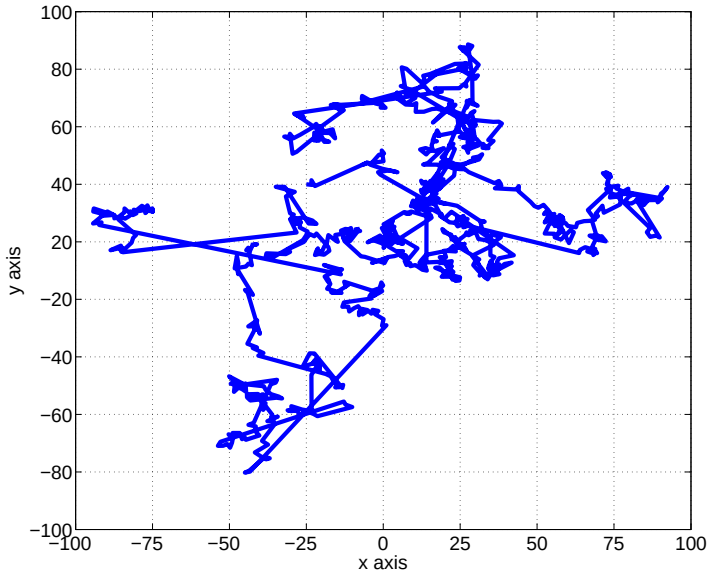
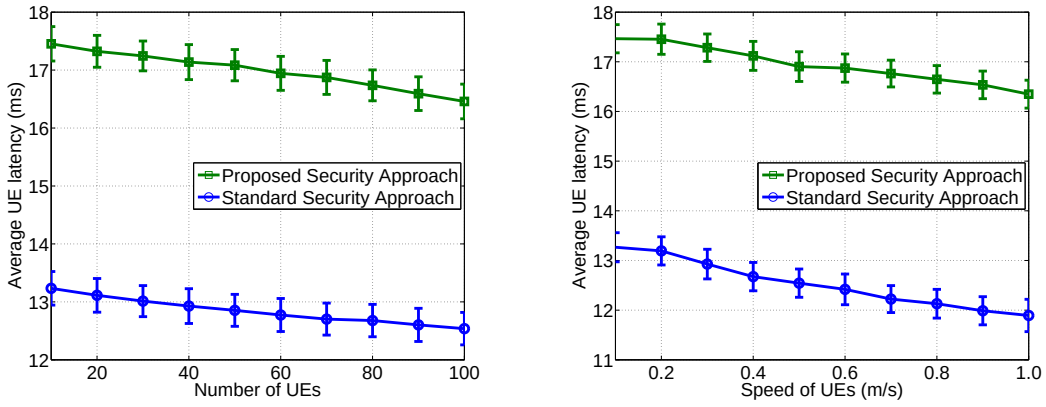


Figure 5.1 *A sample user movement pattern with Levy Flight mobility model*

The simulation environment thus translates into a typical pedestrian scenario, as ratified in the 3GPP specification TS 36.304 [104]. 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 100 MB. The main system parameters are summarized in Table 5.1. The three performance metrics that this work focuses 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 Chapter 4.

Table 5.1 *The main simulation parameters*

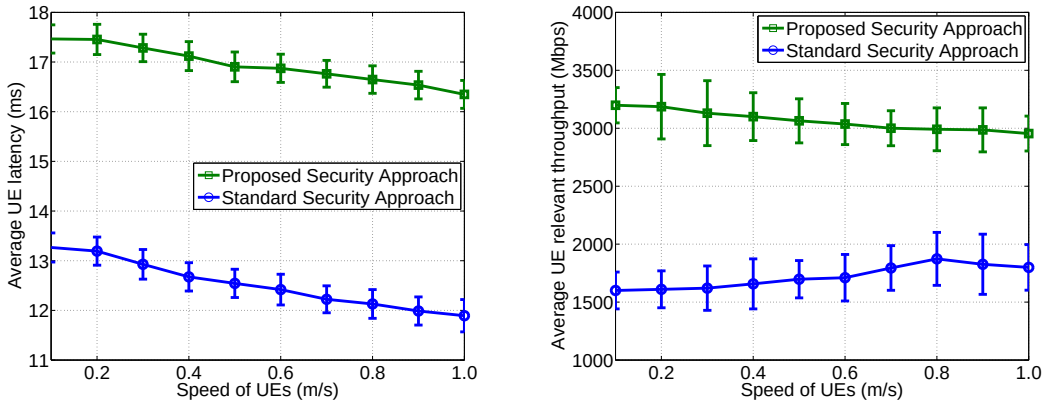
Parameter	**Value**
Cell radius	100 m
Maximum D2D range	30 m
Number of users	20
Target data rate on LTE link	10 Mbps
Target data rate on D2D link	40 Mbps
eNodeB Tx power	46 dBm
UE Tx power	23 dBm
D2D link setup	1 s
Cellular bandwidth	5 MHz
Mobility model	Levy Flight
Simulation time	15 min



(a) Varying the mobility intensity (b) Varying UE speeds

Figure 5.2 *Average user latency (for 100 UEs)*

First, consider the effects of user mobility on the average latency in the proposed framework (see Figures 5.2(a)– 5.3(a)). As one can observe, the latency decreases



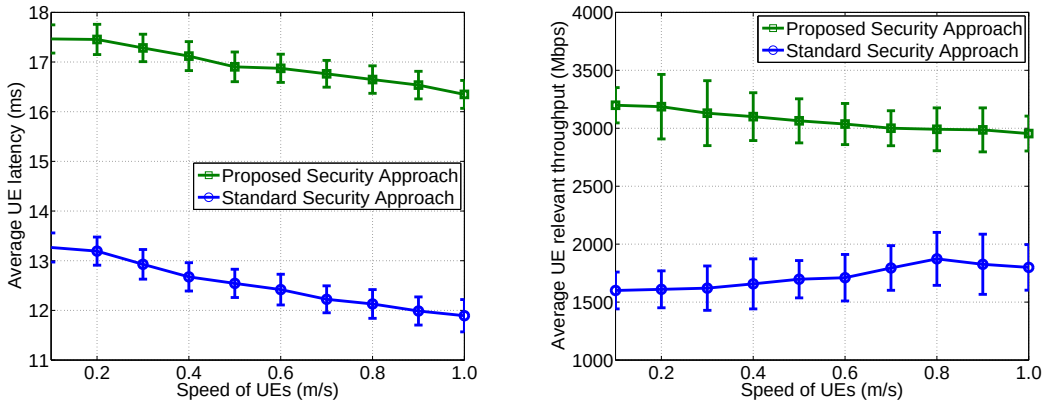
(a) Average UE latency by varying the number of UEs (average speed is 2 m/s)

(b) Average user relevant throughput for varying UE speeds (for 100 UEs)

Figure 5.3 *Average user latency and throughput*

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 a 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 Figure 4.2. 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, the conventional solutions 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 Figure 5.3(b). It is important to note that the proposed security algorithm demonstrates better performance compared to the conventional solution. The reason is that the proposed approach delivers connectivity to users that are in a D2D transmission range, but not under cellular coverage, *Case 3* in Figure 4.2. In this case, the *extra* throughput 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 6.1.



(a) Varying numbers of UEs (b) Varying speeds of UEs

Figure 5.4 *Blocking probability*

Finally, the blocking probability as a function of the number of interrupted download sessions experienced by the users is summarized in Figure 5.4(a) and Figure 5.4(b). As it can be seen in 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 Figure 4.2). 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.

6. PROOF OF THE CONCEPT

In order to conduct a comprehensive study and reveal the practical promises of D2D communications, the author has participated in designing a trial development and deployment program. The trial was aimed at demonstrating how secure direct connectivity paradigm could be when seamlessly integrated into a real-world, operator-grade cellular network with minimal modifications and overheads, as well as within a reasonable time frame. The secondary goal was to quantify the gains that could be achieved by a fully-functional, operator- supported D2D system. To complete these challenging objectives, the implementation team has defined a deployment time constraint of one month and assigned a group of six qualified engineers for the said implementation.

As a basis for the trial, the experimental LTE network of Brno University of Technology (BUT), Czech Republic was used, which supports most of the functionality expected of LTE Release 10 systems. During the trial, the LTE network of BUT was updated with custom implementation of secure direct communications functionality. This has allowed to perform live D2D integration trials, along with corresponding performance evaluations.

6.1 Implementation of the mechanism in live LTE core

In this section, to evaluate the operation of the information security framework, tests in the real-life environment are performed. For the server side, the CentOs virtual machine [105] with two virtual processors Intel(R) Xeon(R) CPU X5472 both running 3.00GHz, 6MB cache size is used. As a mobile device, a Jolla smartphone[1]. running Sailfish OS with Qualcomm Snapdragon 400 1.4 GHz dual-core processor (8930AA) is selected. The comparison of the experimental results for the RSA algorithm using OpenSSL [106] is summarized in Table 6.1. The results obtained

[1]See Jolla smartphone – specification: `https://jolla.com/jolla`

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 6.1 and in more detail in Figure 6.1. In this study, the standard software library available on most of the mobile devices is used, implying that the results can be improved by utilizing specialized lightweight cryptography and hardware on-chip solutions.

Table 6.1 *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

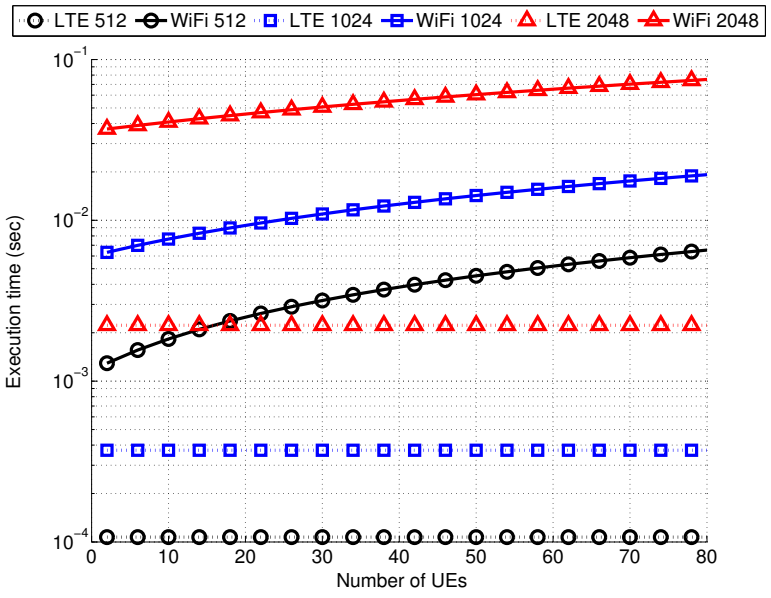


Figure 6.1 *Execution time for a join user procedure ($k = N/2$)*

Further, it was decided to construct a mobile application on top of Android platform testing the feasibility of the security mechanism utilization on the "average" user devices. This application has the functionality of a secure messenger and utilizes the proposed information security primitives. To familiarize the reader with the corresponding framework, the author first outlines the considered network architecture.

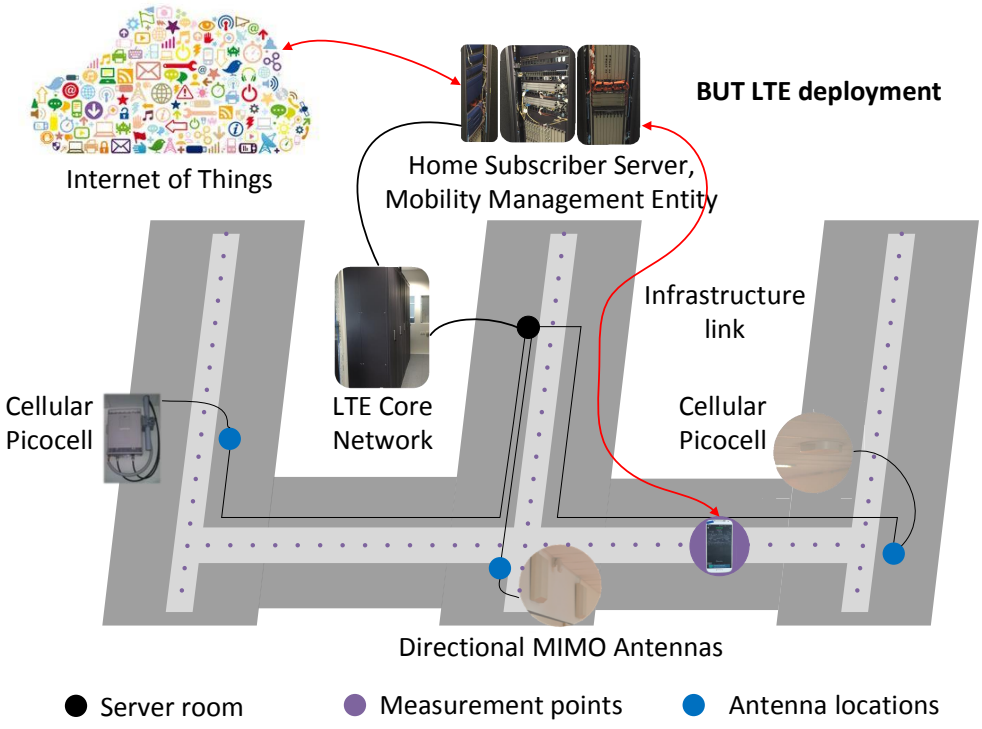


Figure 6.2 *Test 3GPP LTE deployment: structure and main modules*

The experimental 3GPP LTE deployment employed for the purposes of this prototype implementation is located at BUT, Czech Republic. It is a practical, fully-operational cellular infrastructure with all the necessary system modules implemented in hardware. The described LTE testbed (see Figure 6.2) serves the purposes of research and education for 4 years already and its essential components are listed in Table 6.2.

Table 6.2 *Main components of the experimental 3GPP LTE deployment*

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

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

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

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

In case of network-assisted D2D connectivity, IP addresses for users that communicate over a direct channel are also generated by the 3GPP LTE core when it has a reliable link to the corresponding server. For D2D communications outside of cellular coverage, new rules and routing protocols should be constructed. In connection to the above, the effective firewall policies applied inside the cellular network core may restrict direct access from one device to another and hence limit the direct communications opportunities. Therefore, an additional firewall policy to allow for direct connectivity between the cellular network users and the network server was

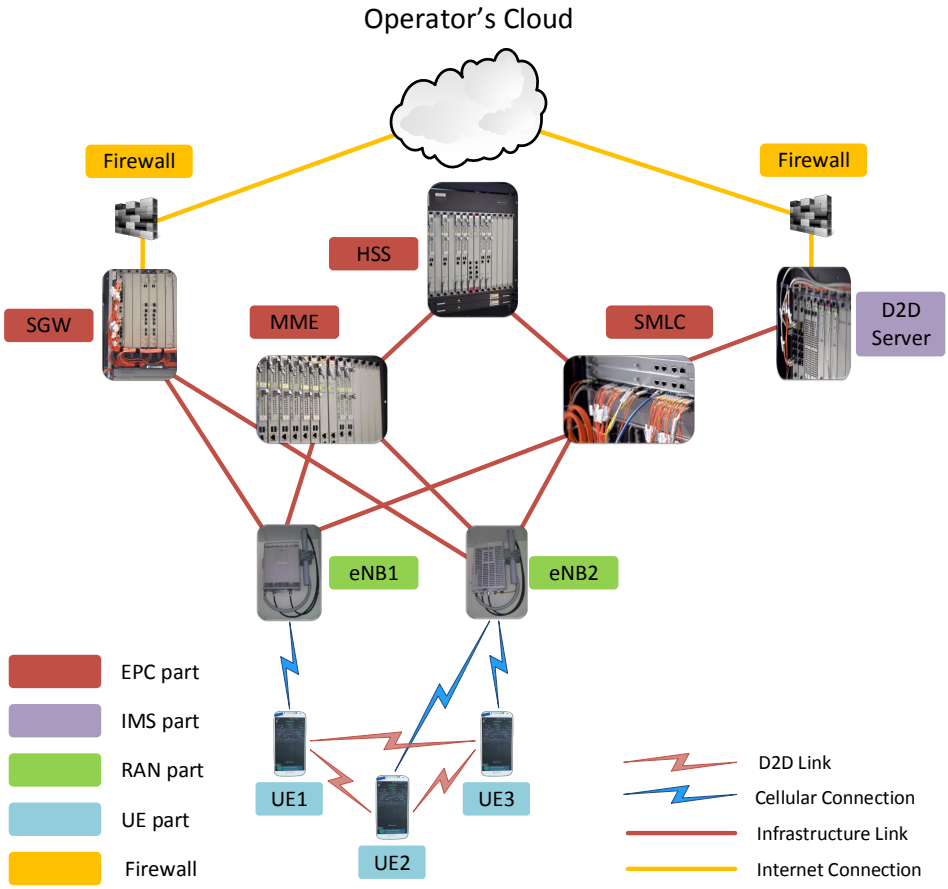


Figure 6.3 *Prototype implementation of a D2D system*

implemented. To this end, the author utilized a specifically-defined port in order to offer the proof of the concept, see Figure 6.3.

For this demo implementation, the LTE system with a server running inside the core is utilized. The D2D server is represented as a Linux machine that has a Python service running in the background. The role of the latter is not only to act as the Certificate Authority (CA), but also manage authentication and logical IP association procedures. We used the Easy-RSA library as a component of the OpenVPN framework for certificate generation. In this demo, the Android-based smart-phones, Samsung Galaxy S4, running non-rooted firmware version 4.4.2. were employed (see Figure 6.4). In the test mobile application, the author of this work implemented a modified Shamir secret sharing scheme focusing on the *java.security.** library. Due to the limitations of WiFi-Direct on Android, the author has decided to use an isolated WiFi AP running OpenWRT to emulate the distributed network.

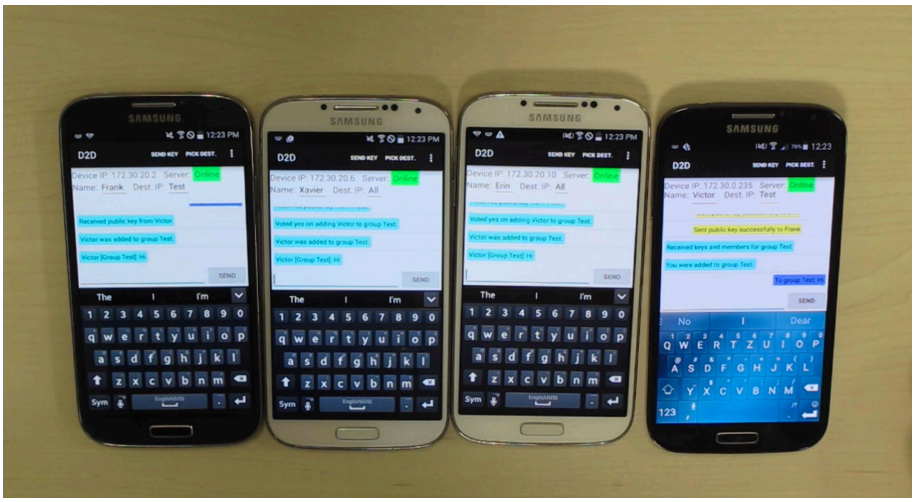


Figure 6.4 *Snapshot of the running demo*

6.2 Integration challenges

In this Section, the author of this thesis discusses the important aspects being faced during the prototype implementation, as well as offers the key numerical results.

In the process of developing this demo, a number of challenges regarding the LTE system operation, networking, and routing on the device side are solved in addition to many smaller issues related to implementing security on Android. Particularly, (i) the effective LTE firewall policies are modified, (ii) a custom routing protocol (LTE to WiFi) is developed and implemented, and (ii) a modified Shamir secret sharing scheme together with all the required modular algebra primitives tailored for Android is constructed.

The main and the most essential learning while working with the real LTE core has been in that its DHCP server was not operating as expected. The devices were assigned IPv4 addresses from the same pool, but from different, random subnets. Clearly, changing the subnetworks on the device side resulted in connectivity failures. To resolve these issues, the author had to additionally conduct thorough traffic analysis to identify the said fault of the network configuration. In the end, LTE IP addresses and subnets have been set statically for each utilized SIM card. However, the community is looking forward to having IPv6 support in next-generation networks, which the author hopes could resolve the routing and identification issues in a more comprehensive way.

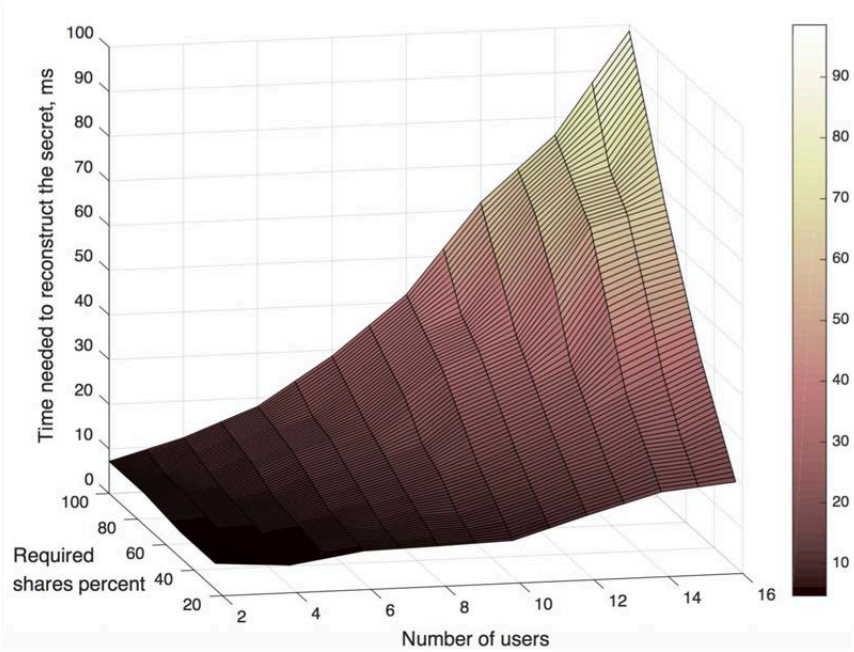


Figure 6.5 *Comparing the time to reconstruct a secret*

Further, the proposed modified Shamir secret sharing scheme has been tested. In particular, the time needed to reconstruct the secret on modern *non-restricted* smart-phones was obtained. The respective results are visualized in Figure 6.5, where one can observe that the proposed scheme is not taking up to 100ms to produce a new point for a newly-joining user or for excluding an existing user from the coalition.

Next, Figure 6.6 highlights the trade-off between the system operational complexity and the selected threshold value of k. Here, the level of trust is indicated in percents – the time of user inclusion/exclusion may vary dramatically as a result of the desired level of trust between the voting users.

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

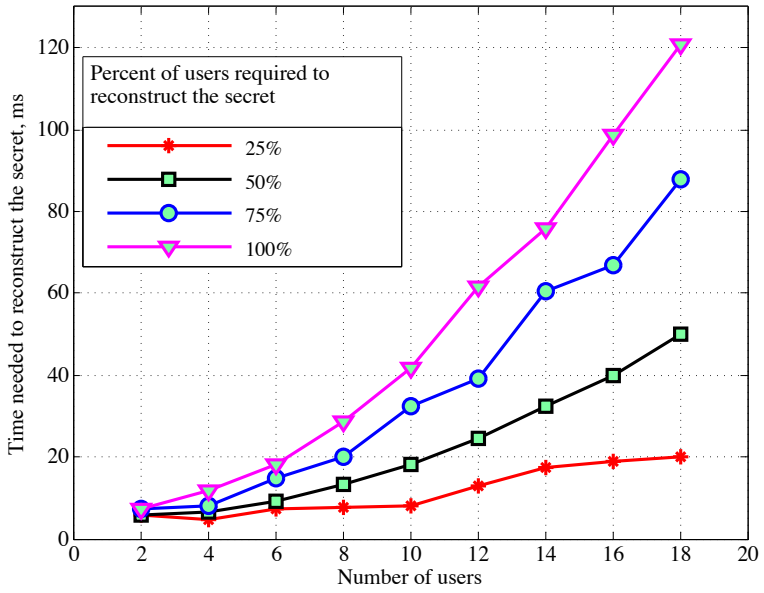


Figure 6.6 *Dependence of the recovery time on the threshold value of k*

6.3 Feasibility study for constrained devices

The Internet of Things (IoT) creates the means for interconnection of highly heterogeneous entities and networks bringing a variety of communications patterns [107]. IoT in general and wearable technology in particular empower the industry to develop new technology in almost unlimited numbers. Today, the term *wearables* stands for connected devices that collect data, track activities and improve user experience across different application domains. From the IoT point of view, wearables could be characterized as networked "smart devices" equipped with microchips, sensors, and wireless communications interfaces deployed in the immediate vicinity of their owner [108].

To prove the feasibility of modern security solutions on the user devices, today's *pioneers* as well as already widely used devices have been selected in accordance to three main categories: (i) smartphones, (ii) smart watches, and (iii) embedded devices, see Figure 6.7.

As representatives of the first group, the author selects devices built on two main mobile platforms: Android and iOS. More specifically, Samsung Galaxy S4 (SGH-

I337) and Jiayu S3 Advanced (JY-S3), both running Android 4.4.2, Apple iPhone 4s (MD128CS/A) running the iOS 7.1.2, and Apple iPhone 6 (MG4F2CN/A) with the latest iOS 9.1 were evaluated.

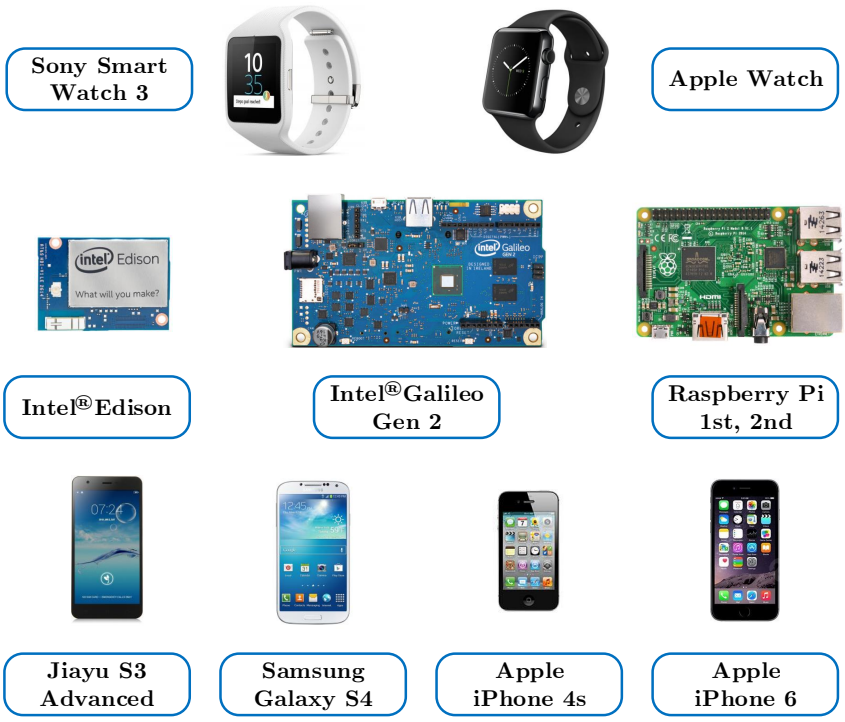


Figure 6.7 *Wearable devices used in this performance evaluation*

To provide a comprehensive evaluation at par with the selected smartphones, the smart watches running Android Wear and Apple WatchOS were also employed. The utilized devices are correspondingly Sony Smart Watch 3 (SWR-50) with Android Wear 5.1.1 and Apple Watch 42mm Sport edition with WatchOS 2.0.

Following the fact that most of today's embedded devices (often named the IoT development boards) are intended to be used also as wearables, the author of this work decided to additionally evaluate the well-known examples from this class: Intel® Edison[2], Raspberry Pi 1 (Model B), and Raspberry Pi 2 (Model B). Both Raspberry Pi devices run the latest version of Raspbian OS (Jessie, v 8.0) together with the latest version of Oracle JDK (1.8.0-b132). Edison features a Ubilinux 3.10.17-yocto-standard-r2 build equipped with JDK (1.8.0_66-b17). In more detail, Edison is a

[2]See Intel® Edison. One Tiny Platform, Endless Possibility: `http://www.intel.de/content/www/de/de/do-it-yourself/edison.html`

small-sized computing module aiming to enable the next generation of wearables and IoT devices, where size and power consumption are extremely important factors. In addition, Edison may be attached to a number of different extension boards, for example, to enable Arduino compatibility. Hence, Edison empowers a range of different use cases, whereas Raspberry Pi might be more suitable for graphics and multimedia related applications and products.

Table 6.3 *Selected devices with their corresponding specifications*

Device	**Type**	**SoC**	**Processor**	**RAM**
Apple Watch	Smart Watch	APL0778	520 MHz Single-core Cortex-A7	512 MB
Sony SmartWatch 3	Smart Watch	BCM47531	1.2 GHz Quad-Core ARM A7	512 MB
Apple iPhone 4s	Smartphone	APL A5	800 MHz Dual-Core Cortex A9 64bit	512 MB
Apple iPhone 6	Smartphone	APL A9	1.5 GHz Dual-Core Cortex A57 64bit	1 GB
Samsung I9500 Galaxy S4	Smartphone	APQ8064T	1.6 GHz Dual-Core Cortex-A15	2 GB
Jiayu S3 Advanced	Smartphone	MT6752	1.7 GHz Octa-Core 64bit Cortex A53	3 GB
Intel® Edison	IoT Dev. Board	Atom + Quark	500 MHz Intel® Atom™ CPU, 100 Mhz MCU	1 GB
Raspberry Pi 1 model B	IoT Dev. Board	BCM2835	700 MHz Single-Core ARM Cortex-A6	512 MB
Raspberry Pi 2 model B	IoT Dev. Board	BCM2836	900 MHz Quad-Core ARM Cortex-A7	1 GB

The following text aims to evaluate the performance of the constrained devices listed in Table 6.3. For Raspberry Pi, Android, and Android Wear devices, the security tests have been executed as a standalone Java application. To run the framework on Apple devices (iPhone 4s, iPhone 6, and Apple Watch), the author has ported the logic and created a standalone application written in Objective-C programming language. To make the assessment conditions even more equivalent, all unnecessary background processes were terminated and the flight mode was utilized whenever possible. To execute the developed application on the restricted Intel® Edison board it was necessary to prepare a Linux build equipped with JRE. Further, an executable jar file was designed, deployed, and executed on the device.

All the tested devices are classified based on their performance metrics into two groups: *Smart devices* and *IoT boards*. As the main user-driven evaluation criterion to characterize this equipment, the security primitive execution time is selected. This is due to the unification and well-acceptance of this approach in addition to the fact that some of the devices are hardware restricted and, therefore, could not provide any other valuable and unified evaluation metric. The following results have been obtained as an average of 1000 executions for each operation to achieve statistically-reliable data.

First, Figure 6.8 indicates the average time overhead for encryption and decryption operations of the conventional non-optimized RSA schemes with correspondence to different decimal digits. Public and private keys were generated using OpenSSL

with default parameters. Adopting a security value of 1024 or 2048 bits and default public exponent (3 bytes) (which is reasonable for the constrained wireless devices [109]), the RSA encryption operation remains under 1 ms on a typical Android smartphone, around 2.5 ms for a Smart Watch, and less than 12 ms on Intel® Edison and Raspberry Pi 2.

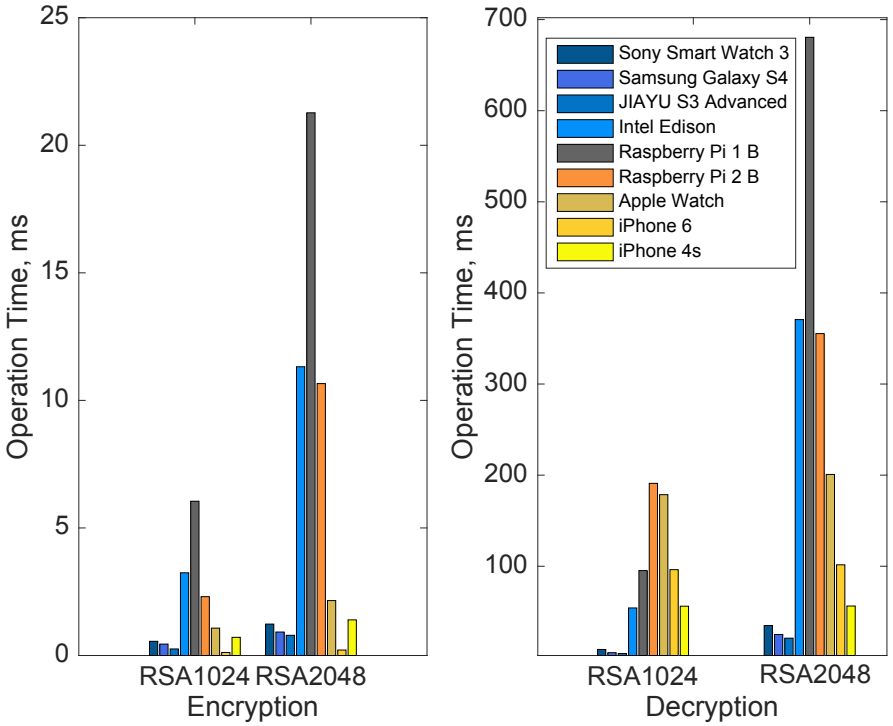


Figure 6.8 *RSA execution time on the IoT device*

Decryption time looks less optimistic and, therefore, for an Android phone it takes around 25 ms, but up to 100 ms for an iPhone. Similar behavior is observed for Android Wear and Apple Watch – here, the values are 35 ms and 200 ms correspondingly. On the IoT boards, the execution may take up to half a second, which may still be feasible for delay-tolerant applications. Concerning smart devices, it can be stated that Sony Watch is demonstrating high performance even though it is not classified as a standalone device. Interestingly, here and further on, iPhone 4s is sometimes showing better results than iPhone 6 or Apple Watch, which may be due to the lack of the power consumption optimization feature on the version of iOS that was introduced only starting 9.0.1. Hence, CPU utilization is able to approach 90 %, while for the latest models it remains well below 50 %.

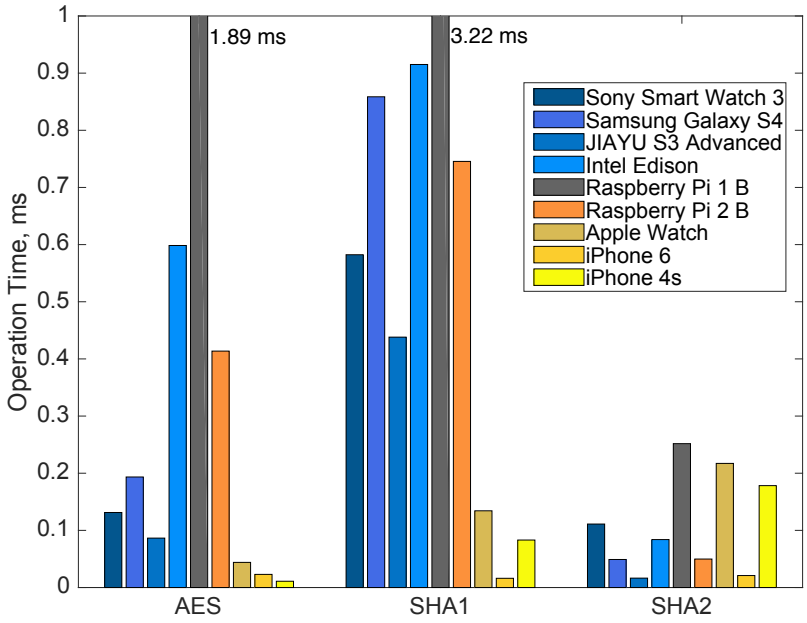


Figure 6.9 *Hashing and AES execution times on the IoT device*

Taking into account such basic operation as Hashing function, the execution of SHA1 and SHA2 (SHA-256) has been evaluated on all of the devices. The corresponding results are summarized in Figure 6.9. It could be concluded that for all of our test devices SHA1 and SHA2 are hardware optimized and mainly depend on the utilized equipment. As an example of the data encryption, the author of this work used AES 128 cipher. The corresponding results still follow the execution time pattern of public-key cryptosystems and hashing functions for all of the chosen devices.

To provide a clear viewpoint of testing, Table 6.4 contains the information of which devices best match which cryptographic operations – with respect to HW parameters in Table 6.3.

Table 6.4 *Suitability of wearables for cryptographic operations over acceptable time*

Device	**Cryptographic operations**
Apple Watch	SHA 1 / 2; Curve operations
Sony SmartWatch 3	RSA 1024, 2048 E / D; Curve operations
Intel® Edison	RSA 2048 E / D; AES; SHA 2
Raspberry Pi 1 model B	RSA 1024 E / D
Raspberry Pi 2 model B	RSA 1024, 2048 E / D; AES; SHA 1

Therefore, the author concludes that modern wearable electronics has already reached the computational power of a two-year-old smartphone and thus the IoT world ful-

fills the security requirements of today. Constrained but powerful IoT devices, like Intel Edison, are designed so that the energy consumption is minimized. Due to that fact, the computational power is somewhat lowered, but this class of devices appears to be an attractive enabler for the required levels of information security. Importantly, the Raspberry Pi board, which is often nicknamed "a tiny and affordable computer" is demonstrating more modest performance results comparing to a small Edison chip designed specifically for the IoT-centric use cases.

7. FUTURE DIRECTIONS

In this Chapter, the author of the manuscript targets to highlight the most essential use cases for direct connectivity in the 5G ecosystem. Currently, the lion's share of the expected mobile traffic growth comes from peer-to-peer services that naturally involve *clients in close proximity* [7] (see Figure 7.1). The potential proximity-based communications also enable shorter and lower-to-the-ground radio links without the cost of additional infrastructure. Hence, we envision that whenever possible the neighboring client devices will use their direct connectivity capabilities, instead of infrastructure (cellular) links. Consequently, D2D connections are anticipated to become an effective solution that would unlock substantial gains in capacity [110] and relieve congestion [9] on the way to 5G mobile networks. For mobile network operators, D2D connectivity is becoming vital to enable *traffic offloading* from the core network and to realize efficient support of social networking through device localization.

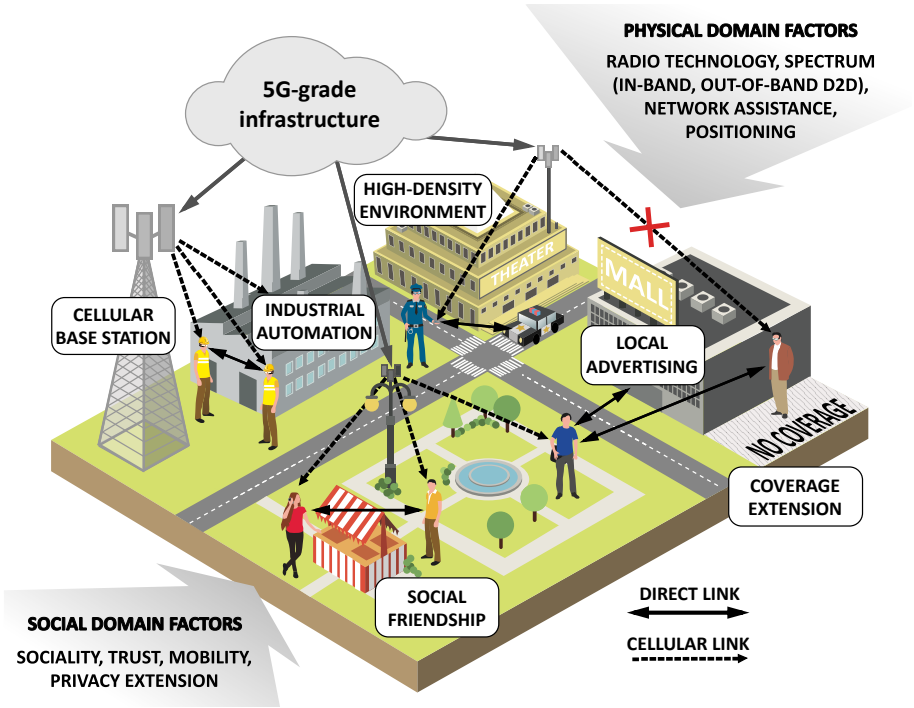


Figure 7.1 *Urban network-assisted D2D applications*

The list of well-studied and novel D2D use cases is as following:

- *Use case 1. Localized traffic offloading.*

  Let us consider a case, where a local media server is setup at a musical festival to offer a substantial amount of promotional material for visitors to download. The phone calls and continuous Internet access for the cellular users should be handled reliably at the same time. The D2D communications may be considered as an effective solution for the local media service access while the cellular connectivity would operate in a conventional way. Moreover, D2D communications may be utilized to upload the data to the media server as well [11].

- *Use case 2. Voluntary cooperation between familiar peers.*

  Mobile phones could be considered as selfish nodes without any default cooperating willingness, i.e. such a node is usually interested in maximizing its own benefit or, more specifically, throughput. Cooperation, in this sense, causes reducing the overall benefits to some extent, i.e. such a cooperation can only be established if fairness is guaranteed among these mobile users [7].

- *Use case 3. Discovery of new (unfamiliar) people and services.*

  Promoted by Qualcomm [111], this scenario includes content sharing and multiplayer gaming in addition to location-based advertising [27].

- *Use case 4. Public Protection and Disaster Relief (PPDR) scenarios.*

  In a national security and public safety situation or outside of cellular coverage, cellular mobile devices could communicate without network assistance, similarly to the Terrestrial Trunked Radio (TETRA) technology [10].

- *Use case 5. Caching of multimedia content.*

  Since modern mobile devices have large built-in memory resources, they can effectively act as wireless caching stations. In this case, no additional infrastructure deployment is required and the substantial possible advantage of the stations with this feature enabled is by being concentrated in those areas where the highest demand occurs. The data transfer between the caching node and a regular device essentially becomes “device-to-device” communications [67].

- *Use case 6. D2D-based multihop relaying (potential use of network coding).*

  It is proposed that by selecting an appropriate initial pushing set of seeds and utilizing D2D sharing, content can be disseminated efficiently while cellular traffic can be reduced significantly [112].

- *Use case 7. Wearable technology.*

  Knowing the fact that the smart wearable market's global retail revenue will triple by 2016, eventually reaching $53.2 billion by 2019, compared to the $4.5 billion at the end of 2015 [113], the author stresses the need for controllable interference also for the wearable devices [114].

The author of this work has listed just a few examples of the secure direct connectivity scenarios. In the world of today, we are only limited by our imagination in proposing those. On the other hand, as the technology is mainly driven by industry, the proper standardization activities are required to support its growth.

8. CONCLUSIONS

This Chapter concludes the thesis with a review of several important topics. Proximity based communications is one of the key technologies within the rapidly maturing 5G ecosystem that would broadly enable both the owners of advanced wireless devices as well as the smart and social IoT objects across diverse, pervasive platforms to effectively become a part of the cellular landscape. This, in turn, will pave the way to improved cellular service provisioning by e.g., offering D2D-based data relaying, content distribution and caching, or other forms of cooperative communications to augment the existing spectrum usage and device energy efficiency. Another exciting research direction is to develop new mechanisms that take advantage of the unique position of cellular operators – with their well-developed infrastructure and pricing methods – to create incentives, win-win collaborative strategies, and ultimately raise social awareness among spectrum owners, network operators, and wireless device users. For 3GPP networks, the basic building blocks, associated protocol structures, and physical layer procedures are already being defined, while the creation of corresponding incentives and social awareness schemes that engage users as part of the service provisioning effort remains in strong need of further research.

This thesis demonstrated application of combined de-/centralized networking concept utilization in implementing prototypes and demonstrators for emerging wireless network architectures. Started with technological background and followed by anticipated development challenges, the proposed security approach demonstrated an implementation possibility for considered industry-driven scenarios including conventional and constrained devices involved. Particularly, the proposed information security framework, simulation results, and implemented prototype supporting the corresponding research resulted in several journal and conference publications. Feasibility of the implemented secure network assisted communications for D2D traffic was also validated during full-scale practical trial on a live network deployment.

BIBLIOGRAPHY

[1] A. Ometov, A. Orsino, L. Militano, G. Araniti, D. Moltchanov, and S. Andreev, "A Novel Security-Centric Framework for D2D Connectivity Based on Spatial and Social Proximity," *Computer Networks*, 2016.

[2] A. Asadi, Q. Wang, and V. Mancuso, "A Survey on Device-to-Device Communication in Cellular Networks," *IEEE Communications Surveys & Tutorials*, vol. 16, no. 4, pp. 1801–1819, 2014.

[3] N. Bhushan, J. Li, D. Malladi, R. Gilmore, D. Brenner, A. Damnjanovic, R. Sukhavasi, C. Patel, and S. Geirhofer, "Network Densification: The Dominant Theme for Wireless Evolution into 5G," *IEEE Communications Magazine*, vol. 52, pp. 82–89, 2014.

[4] M. Mirahsan, R. Schoenen, H. Yanikomeroglu, G. Senarath, and N. Dung-Dao, "User-in-the-loop for HetHetNets with backhaul capacity constraints," *IEEE Wireless Communications*, vol. 22, no. 5, pp. 50–57, 2015.

[5] R. Schoenen, H. U. Sokun, and H. Yanikomeroglu, "Effective quantum (eBit) tariff – A novel approach to enable smart data pricing," *IEEE Network Magazine, Special Issue on Smart Data Pricing*, August 2015.

[6] B. Zhang, Y. Li, D. Jin, P. Hui, and Z. Han, "Social-Aware Peer Discovery for D2D Communications Underlaying Cellular Networks," *IEEE Transactions on Wireless Communications*, vol. 14, no. 1, pp. 177–190, 2015.

[7] 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.

[8] S. Andreev, D. Moltchanov, O. Galinina, A. Pyattaev, A. Ometov, and 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.

[9] C.-H. Yu, K. Doppler, C. B. Ribeiro, and O. Tirkkonen, "Resource sharing optimization for device-to-device communication underlaying cellular networks,"

IEEE Transactions on Wireless Communications, vol. 10, no. 8, pp. 2752–2763, 2011.

[10] G. Fodor, E. Dahlman, G. Mildh, S. Parkvall, N. Reider, G. Miklós, and Z. Turányi, "Design aspects of network assisted device-to-device communications," *IEEE Communications Magazine*, vol. 50, no. 3, pp. 170–177, 2012.

[11] K. Doppler, M. Rinne, C. Wijting, C. B. Ribeiro, and K. Hugl, "Device-to-device communication as an underlay to LTE-advanced networks," *IEEE Communications Magazine*, vol. 47, no. 12, pp. 42–49, 2009.

[12] L. Al-Kanj, Z. Dawy, W. Saad, and E. Kutanoglu, "Energy-aware cooperative content distribution over wireless networks: Optimized and distributed approaches," *IEEE Transactions on Vehicular Technology*, vol. 62, no. 8, pp. 3828–3847, 2013.

[13] D. Feng, L. Lu, Y. Yuan-Wu, G. Y. Li, G. Feng, and S. Li, "Device-to-device communications underlaying cellular networks," *IEEE Transactions on Communications*, vol. 61, no. 8, pp. 3541–3551, 2013.

[14] X. Lin, J. Andrews, and A. Ghosh, "Spectrum sharing for device-to-device communication in cellular networks," *IEEE Transactions on Wireless Communications*, 2013.

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

[16] S. Xu, H. Wang, T. Chen, T. Peng, and K. S. Kwak, "Device-to-Device Communication Underlaying Cellular Networks: Connection Establishment and Interference Avoidance," *KSII Transactions on Internet & Information Systems*, vol. 6, no. 1, 2012.

[17] H. Min, W. Seo, J. Lee, S. Park, and D. Hong, "Reliability improvement using receive mode selection in the device-to-device uplink period underlaying cellular networks," *IEEE Transactions on Wireless Communications*, vol. 10, no. 2, pp. 413–418, 2011.

[18] D. Wu, L. Zhou, Y. Cai, R. Q. Hu, and Y. Qian, "The role of mobility for D2D communications in LTE-Advanced networks: energy vs. bandwidth efficiency," *IEEE Wireless Communications*, vol. 21, no. 2, pp. 66–71, 2014.

[19] K. Huang, V. K. Lau, and Y. Chen, "Spectrum sharing between cellular and mobile ad hoc networks: transmission-capacity trade-off," *IEEE Journal on Selected Areas in Communications*, vol. 27, no. 7, pp. 1256–1267, 2009.

[20] P. Pahlevani, M. Hundeboll, M. V. Pedersen, D. Lucani, H. Charaf, F. Fitzek, H. Bagheri, and M. Katz, "Novel concepts for device-to-device communication using network coding," *IEEE Communications Magazine*, vol. 52, no. 4, pp. 32–39, 2014.

[21] 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*, 2015.

[22] X. Lin, J. G. Andrews, A. Ghosh, and R. Ratasuk, "An overview of 3GPP device-to-device proximity services," *IEEE Communications Magazine*, vol. 52, no. 4, pp. 40–48, 2014.

[23] D. Astely, E. Dahlman, G. Fodor, S. Parkvall, and J. Sachs, "LTE Release 12 and Beyond," *IEEE Communications Magazine*, vol. 51, no. 7, pp. 154–160, 2013.

[24] A. Vigato, L. Vangelista, C. Measson, and X. Wu, "Joint discovery in synchronous wireless networks," *IEEE Transactions on Communications*, vol. 59, no. 8, pp. 2296–2305, 2011.

[25] H. ElSawy, E. Hossain, and M. Alouini, "Analytical modeling of mode selection and power control for underlay D2D communication in cellular networks," *IEEE Transactions on Communications*, vol. 62, no. 11, pp. 4147–4161, 2014.

[26] P. Phunchongharn, E. Hossain, and D. I. Kim, "Resource allocation for device-to-device communications underlaying LTE-advanced networks," *IEEE Wireless Communications*, vol. 20, no. 4, pp. 91–100, 2013.

[27] L. Lei, Z. Zhong, C. Lin, and X. Shen, "Operator controlled device-to-device communications in LTE-advanced networks," *IEEE Wireless Communications*, vol. 19, no. 3, p. 96, 2012.

[28] A. Pyattaev, O. Galinina, S. Andreev, M. Katz, and Y. Koucheryavy, "Understanding Practical Limitations of Network Coding for Assisted Proximate

Communication," *IEEE Journal on Selected Areas in Communications*, vol. 33, no. 2, pp. 156–170, 2015.

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

[30] S. Andreev, A. Pyattaev, K. Johnsson, O. Galinina, and Y. Koucheryavy, "Cellular traffic offloading onto network-assisted device-to-device connections," *IEEE Communications Magazine*, vol. 52, no. 4, pp. 20–31, 2014.

[31] G. Fodor, S. Sorrentino, and S. Sultana, "Network Assisted Device-to-Device Communications: Use Cases, Design Approaches, and Performance Aspects," in *Smart Device to Smart Device Communication.* Springer, 2014, pp. 135–163.

[32] 3GPP TR 22.803, "Feasibility Study for Proximity Services (ProSe)," Release 12, Tech. Rep., 2013.

[33] 3GPP TR 22.703, "Study on architecture enhancements to support Proximity Services (ProSe)," Tech. Rep., Mar. 2012.

[34] 3GPP TS 36.843, "Study on LTE device to device proximity services; radio aspects," Release 12, 2014.

[35] L. Wei, R. Q. Hu, Y. Qian, and G. Wu, "Enable device-to-device communications underlaying cellular networks: challenges and research aspects," *IEEE Communications Magazine*, vol. 52, no. 6, pp. 90–96, 2014.

[36] M. J. Yang, S. Y. Lim, H. J. Park, and N. H. Park, "Solving the data overload: Device-to-device bearer control architecture for cellular data offloading," *IEEE Vehicular Technology Magazine*, vol. 8, no. 1, pp. 31–39, 2013.

[37] L. Wei, R. Hu, Y. Qian, and G. Wu, "Key elements to enable millimeter wave communications for 5G wireless systems," *IEEE Wireless Communications*, vol. 21, no. 6, pp. 136–143, 2014.

[38] R. Schoenen and H. Yanikomeroglu, "User-in-the-loop: spatial and temporal demand shaping for sustainable wireless networks," *IEEE Communications Magazine*, vol. 52, no. 2, pp. 196–203, 2014.

[39] *LTE Direct Always-on Device-to-Device Proximal Discovery*, Qualcomm Technologies, 2014.

[40] K. J. Zou, M. Wang, K. W. Yang, J. Zhang, W. Sheng, Q. Chen, and X. You, "Proximity discovery for device-to-device communications over a cellular network," *IEEE Communications Magazine*, vol. 52, no. 6, pp. 98–107, 2014.

[41] L. Lei, Y. Kuang, X. Shen, C. Lin, and Z. Zhong, "Resource control in network assisted device-to-device communications: solutions and challenges," *IEEE Communications Magazine*, vol. 52, no. 6, pp. 108–117, 2014.

[42] Q. Ye, M. Al-Shalash, C. Caramanis, and J. G. Andrews, "Distributed resource allocation in device-to-device enhanced cellular networks," *IEEE Transactions on Communications*, vol. 63, no. 2, pp. 441–454, 2015.

[43] H. Nishiyama, M. Ito, and N. Kato, "Relay-by-smartphone: realizing multihop device-to-device communications," *IEEE Communications Magazine*, vol. 52, no. 4, pp. 56–65, 2014.

[44] "WINTERsim system-level simulator description," http://winter-group.net/downloads/, January 2016.

[45] A. Laya, K. Wang, A. A. Widaa, J. Alonso-Zarate, J. Markendahl, and L. Alonso, "Device-to-device communications and small cells: enabling spectrum reuse for dense networks," *IEEE Wireless Communications*, vol. 21, no. 4, pp. 98–105, 2014.

[46] S. Andreev, A. Pyattaev, K. Johnsson, O. Galinina, and Y. Koucheryavy, "Network-Assisted Offloading of Cellular Data Sessions onto Device-to-Device Connections," *IEEE Journal on Selected Areas in Communications*, 2015.

[47] W. Wang and V. K. Lau, "Delay-aware cross-layer design for device-to-device communications in future cellular systems," *IEEE Communications Magazine*, vol. 52, no. 6, pp. 133–139, 2014.

[48] B. Zhou, H. Hu, S.-Q. Huang, and H.-H. Chen, "Intracluster device-to-device relay algorithm with optimal resource utilization," *IEEE Transactions on Vehicular Technology*, vol. 62, no. 5, pp. 2315–2326, 2013.

[49] L. Militano, M. Condoluci, G. Araniti, A. Molinaro, and A. Iera, "When D2D communication improves group oriented services in beyond 4G networks," *Wireless Networks*, November 2014.

[50] L. Militano, M. Condoluci, G. Araniti, A. Molinaro, A. Iera, and F. Fitzek, "Wi-Fi cooperation or D2D-based multicast content distribution in LTE-A: A comparative analysis," in *ICC Workshops*, 2014.

[51] M. Condoluci, L. Militano, G. Araniti, A. Molinaro, and A. Iera, "Multicasting in LTE-A networks enhanced by device-to-device communications," in *Globecom Workshops*, 2014.

[52] X. Lin, R. Ratasuk, A. Ghosh, and J. G. Andrews, "Modeling, analysis and optimization of multicast device-to-device transmissions," *IEEE Transactions on Wireless Communications*, vol. 13, no. 8, pp. 4346–4359, 2014.

[53] D. Moltchanov, M. Gerasimenko, Q. Wang, S. Andreev, and Y. Koucheryavy, "On the Optimal Assisted Rate Allocation in N-Tier Multi-RAT Heterogeneous Networks," in *IEEE PIMRC*, 2014, pp. 1525–1530.

[54] L. Song, D. Niyato, Z. Han, and E. Hossain, "Game-theoretic resource allocation methods for device-to-device communication," *IEEE Wireless Communications*, vol. 21, no. 3, pp. 136–144, 2014.

[55] X. Lu, P. Wang, and D. Niyato, "Hierarchical cooperation for operator-controlled device-to-device communications: A layered coalitional game approach," in *Proc. of IEEE Wireless Communications and Networking Conference (WCNC)*. IEEE, 2015, pp. 2056–2061.

[56] Y. Li, C. Song, D. Jin, and S. Chen, "A dynamic graph optimization framework for multihop device-to-device communication underlaying cellular networks," *IEEE Wireless Communications*, vol. 21, no. 5, pp. 52–61, 2014.

[57] A. H. Sakr and E. Hossain, "Cognitive and energy harvesting-based d2d communication in cellular networks: Stochastic geometry modeling and analysis," *IEEE Transactions on Communications*, vol. 63, no. 5, pp. 1867–1880, 2015.

[58] O. Galinina, S. Andreev, M. Gerasimenko, Y. Koucheryavy, N. Himayat, S. Yeh, and S. Talwar, "Capturing Spatial Randomness of Heterogeneous Cellular/WLAN Deployments With Dynamic Traffic," *IEEE Journal on Selected Areas in Communications*, vol. 32, pp. 1083–1099, 2014.

[59] S. Andreev, M. Gerasimenko, O. Galinina, Y. Koucheryavy, N. Himayat, S. Yeh, and S. Talwar, "Intelligent Access Network Selection in Converged

Multi-Radio Heterogeneous Networks," *IEEE Wireless Communications Magazine*, vol. 21, pp. 86–96, 2014.

[60] J. Silva, G. Fodor, and T. Maciel, "Performance Analysis of Network-Assisted Two-Hop D2D Communications," in *GLOBECOM Workshops*, 2014, pp. 1050–1056.

[61] J. G. Andrews, "Seven ways that HetNets are a cellular paradigm shift," *IEEE Communications Magazine*, vol. 51, no. 3, pp. 136–144, 2013.

[62] A. Aijaz, H. Aghvami, and M. Amani, "A survey on mobile data offloading: technical and business perspectives," *IEEE Wireless Communications*, vol. 20, no. 2, pp. 104–112, 2013.

[63] A. T. Gamage, H. Liang, R. Zhang, and X. Shen, "Device-to-device communication underlaying converged heterogeneous networks," *IEEE Wireless Communications*, vol. 21, no. 6, pp. 98–107, 2014.

[64] Cisco, "Cisco Visual Networking Index: Global Mobile Data Traffic Forecast Update, 2015–2020," February 2016.

[65] J. Liu, Y. Kawamoto, H. Nishiyama, N. Kato, and N. Kadowaki, "Device-to-device communications achieve efficient load balancing in LTE-advanced networks," *IEEE Wireless Communications*, vol. 21, no. 2, pp. 57–65, 2014.

[66] F. Boccardi, R. W. Heath Jr, A. Lozano, T. L. Marzetta, and P. Popovski, "Five Disruptive Technology Directions for 5G," *IEEE Communications Magazine*, vol. 52, no. 2, pp. 74–80, 2014.

[67] N. Golrezaei, A. F. Molisch, A. G. Dimakis, and G. Caire, "Femtocaching and device-to-device collaboration: A new architecture for wireless video distribution," *IEEE Communications Magazine*, vol. 51, no. 4, pp. 142–149, 2013.

[68] L. Jin, Y. Chen, T. Wang, P. Hui, and A. V. Vasilakos, "Understanding user behavior in online social networks: A survey," *IEEE Communications Magazine*, vol. 51, no. 9, pp. 144–150, 2013.

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

[70] Q. Lu, Q. Miao, G. Fodor, and N. Brahmi, "Clustering Schemes for D2D Communications under Partial/No Network Coverage," in *Proc. of IEEE 79th Vehicular Technology Conference (VTC Spring)*. IEEE, 2014, pp. 1–5.

[71] 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.

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

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

[74] M. N. Johnstone and 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.

[75] A. Khalili, J. Katz, and W. A. Arbaugh, "Toward secure key distribution in truly ad-hoc networks," in *Proc. of Symposium on Applications and the Internet Workshops*. IEEE, 2003, pp. 342–346.

[76] X. Yi, J. Willemson, and F. Nait-Abdesselam, "Privacy-Preserving Wireless Medical Sensor Network," in *Proc. of 12th IEEE International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom)*. IEEE, 2013, pp. 118–125.

[77] D. B. Johnson and D. A. Maltz, "Dynamic source routing in ad hoc wireless networks," in *Mobile computing*. Springer, 1996, pp. 153–181.

[78] Y. Wang, Z. Chen, Y. Yao, M. Shen, and B. Xia, "Secure communications of cellular users in device-to-device communication underlaying cellular networks," in *Proc. of Sixth International Conference on Wireless Communications and Signal Processing (WCSP)*. IEEE, 2014, pp. 1–6.

[79] W. Shen, W. Hong, X. Cao, B. Yin, D. M. Shila, and Y. Cheng, "Secure key establishment for device-to-device communications," in *Proc. of IEEE Global Communications Conference*. IEEE, 2014, pp. 336–340.

[80] D. Zhu, A. L. Swindlehurst, S. A. A. Fakoorian, W. Xu, and C. Zhao, "Device-to-device communications: The physical layer security advantage," in *Proc. of IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*. IEEE, 2014, pp. 1606–1610.

[81] A. Perrig, J. Stankovic, and D. Wagner, "Security in wireless sensor networks," *Communications of the ACM*, vol. 47, no. 6, pp. 53–57, 2004.

[82] P. McDaniel and S. McLaughlin, "Security and privacy challenges in the smart grid," *IEEE Security & Privacy*, vol. 7, no. 3, pp. 75–77, 2009.

[83] J.-P. Hubaux, S. Capkun, and J. Luo, "The security and privacy of smart vehicles," *IEEE Security & Privacy Magazine*, vol. 2, no. LCA-ARTICLE-2004-007, pp. 49–55, 2004.

[84] W. Diffie and M. E. Hellman, "New Directions in Cryptography," *IEEE Transactions on Information Theory*, vol. 22, no. 6, pp. 644–654, 1976.

[85] D. Liu, P. Ning, and R. Li, "Establishing Pairwise Keys in Distributed Sensor Networks," *ACM Transactions on Information and System Security (TISSEC)*, vol. 8, no. 1, pp. 41–77, 2005.

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

[87] A. Perrig, R. Szewczyk, J. Tygar, V. Wen, and D. E. Culler, "SPINS: Security protocols for sensor networks," *Wireless networks*, vol. 8, no. 5, pp. 521–534, 2002.

[88] W. Du, J. Deng, Y. S. Han, P. K. Varshney, J. Katz, and A. Khalili, "A pairwise key predistribution scheme for wireless sensor networks," *ACM Transactions on Information and System Security (TISSEC)*, vol. 8, no. 2, pp. 228–258, 2005.

[89] S. Zhu, S. Setia, and S. Jajodia, "LEAP+: Efficient security mechanisms for large-scale distributed sensor networks," *ACM Transactions on Sensor Networks (TOSN)*, vol. 2, no. 4, pp. 500–528, 2006.

[90] P. Zimmermann, "Why I Wrote PGP," *//Part of the Original.*, June 1991.

[91] L. Zhou and Z. J. Haas, "Securing ad hoc networks," *IEEE Network*, vol. 13, no. 6, pp. 24–30, 1999.

[92] X. Du, Y. Wang, J. Ge, and Y. Wang, "An ID-based broadcast encryption scheme for key distribution," *IEEE Transactions on Broadcasting*, vol. 51, no. 2, pp. 264–266, 2005.

[93] G.-H. Chiou and W.-T. Chen, "Secure broadcasting using the secure lock," *IEEE Transactions on Software Engineering*, vol. 15, no. 8, pp. 929–934, 1989.

[94] T. Jakobsen and L. R. Knudsen, "The interpolation attack on block ciphers," in *Fast Software Encryption*. Springer, 1997, pp. 28–40.

[95] R. J. McEliece and D. V. Sarwate, "On Sharing Secrets and Reed-Solomon Codes," *Communications of the ACM*, vol. 24, no. 9, pp. 583–584, 1981.

[96] C. W. Man and R. Safavi-Naini, "Democratic key escrow scheme," in *Information Security and Privacy*. Springer, 1997, pp. 249–260.

[97] J. Yuan and C. Ding, "Secret sharing schemes from three classes of linear codes," *IEEE Transactions on Information Theory*, vol. 52, no. 1, pp. 206–212, 2006.

[98] J. L. Massey, "Minimal codewords and secret sharing," in *Proc. of the 6th Joint Swedish-Russian International Workshop on Information Theory*. Citeseer, 1993, pp. 276–279.

[99] R. McEliece, "A Public-Key Cryptosystem Based on Algebraic Coding Theory," *DSN Progress Report*, pp. 42–44, January - February 1978.

[100] M. Narasimha, G. Tsudik, and J. H. Yi, "On the utility of distributed cryptography in P2P and MANETs: the case of membership control," in *Proc. of 11th IEEE International Conference on Network Protocols.* IEEE, 2003, pp. 336–345.

[101] D. Brockmann, L. Hufnagel, and T. Geisel, "The scaling laws of human travel," *Nature*, vol. 439, pp. 462–465, 2006.

[102] M. C. Gonzalez, C. A. Hidalgo, and A.-L. Barabasi, "Understanding individual human mobility patterns," *Nature*, vol. 453, pp. 779—782, 2008.

[103] I. Rhee, M. Shin, S. Hong, K. Lee, S. J. Kim, and S. Chong, "On the levy-walk nature of human mobility," *IEEE/ACM transactions on networking (TON)*, vol. 19, no. 3, pp. 630–643, 2011.

[104] 3GPP TS 36.304, "User Equipment (UE) procedures in idle mode (E-UTRAN)," Release 8, 209.

[105] C. Negus and T. Boronczyk, *CentOS Bible*. Wiley Publishing, 2009.

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

[107] A. Ometov, P. Masek, L. Malina, R. Florea, J. Hosek, S. Andreev, J. Hajny, J. Niutanen, and Y. Koucheryavy, "Feasibility characterization of cryptographic primitives for constrained (wearable) IoT devices," in *2016 IEEE International Conference on Pervasive Computing and Communication Workshops (PerCom Workshops)*. IEEE, 2016, pp. 1–6.

[108] A. D. Thierer, "The Internet of Things and Wearable Technology: Addressing Privacy and Security Concerns without Derailing Innovation," *Rich. JL & Tech.*, vol. 21, pp. 6–15, 2015.

[109] M. Brown, D. Cheung, D. Hankerson, J. L. Hernandez, M. Kirkup, and A. Menezes, "PGP in Constrained Wireless Devices," in *USENIX Security Symposium*, 2000.

[110] A. Ozgur, O. Lévêque, and D. N. Tse, "Hierarchical cooperation achieves optimal capacity scaling in ad hoc networks," *IEEE Transactions on Information Theory*, vol. 53, no. 10, pp. 3549–3572, 2007.

[111] S. Turtinen, S.-J. Hakola, and T. K. Koskela, "Discovery in device-to-device communication," Nov. 19 2013, uS Patent 8,588,690.

[112] X. Wang, M. Chen, T. Kwon, L. Jin, and V. Leung, "Mobile traffic offloading by exploiting social network services and leveraging opportunistic device-to-device sharing," *IEEE Wireless Communications*, vol. 21, no. 3, pp. 28–36, 2014.

[113] M. S. Whitcup and K. LaMattina, "Juniper – What is Inhibiting Growth in the Medical Device Wearable Market?" September 2014.

[114] A. Pyattaev, K. Johnsson, S. Andreev, and Y. Koucheryavy, "Communication Challenges in High-Density Deployments of Wearable Wireless Devices," *IEEE Wireless Communications Magazine*, vol. 22, no. 1, pp. 12–18, 2015.