IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 5, Issue 7, July 2016

LTE Direct as a Device-to-Device Network Technology: Use Cases and Security

Umut Can Çabuk[1], Georgios Kanakis[2], Ferişţah Dalkılıç[3]

Department of Electronics Engineering, Erzincan University, Erzincan, Turkey [1]

Johannes Kepler University, Institute of Software Systems Engineering, Linz, Austria [2]

Dokuz Eylul University, Department of Computer Engineering, Izmir, Turkey [3]

Abstract: While the Internet is evolving to the Internet of Things, all other technologies that are related to it are also advancing in a way to contain and support concepts like device-to-device networking, proximate discovery, energy efficiency and security. One of the fastest thrives can be seen in mobile communication technologies. This became more obvious after 4G spread out. In our study, we present a review of a new and revolutionary mobile technology under development: LTE Direct; which runs on licensed radio spectrum and is claimed to be energy efficient and secure, while enabling new approaches for the Internet of Things. We state why and how LTE Direct should replace existing systems, by making an analysis considering provided features, resource consumption, possible use cases and security concerns, as well as comparisons with the conventional technologies. Lastly, we provide ideas for the areas where further research should be made to have this system be a reality.

Keywords: LTE Direct, Device-to-Device Networking, Internet of Things, Proximate Discovery, Energy Efficiency.

I. INTRODUCTION

A few years ago, in late 2000s, Device-to-Device networks start raising upon portable devices and mobile phones via the introduction of Bluetooth (BT) [1] and WiFi [2]. At that point, the mobile operators did not take any action and had no interest in utilizing this new trend [3], of course the main reason was the usage of free ISM radio bands. Users could, now, be connected to each other without the need of mobile operators. A huge revolution begun in short while where devices equipped with BT and/or WiFi availability as well as other emerging technologies like radio-frequency identification (RFID) and near field communication (NFC), plus IPv6 penetration, showed that the internet of things could be close enough. At the same time, the new 4G mobile network was introduced and the LTE was developing, this gave the opportunity for the mobile operators to switch their attention towards device-to-device networks and proximate discovery. After several years of work with FlashlinQ [4], LTE Direct was proposed and a submission for study item was made to 3GPP by Qualcomm at August 2011 [5]. It is claimed to outreach current solutions by its energy efficiency, sustainable band allocation and security [6]. Moreover, the context and location aware applications created space for LTE Direct to be used in a wide variety of cases providing the necessary security over the previous existing technologies.

In this paper, in section 2 we provide background information about the technologies discussed, then, in section 3, we provide an analysis of the advantages of the LTE in comparison with WiFi and BT. We, also, provide the cases where the LTE Direct could be used by surpassing current systems, the pros and cons of the technology and the security risks that are involved and how they are treated. Finally, in section 4, we give our concluding comments for this new emerging technology and we provide suggestions for future work and research in fields that we believe could be interesting for further investigation.

II. BACKGROUND

A. Device-to-Device Networks

Device to Device communication (D2D) is given by the notion of devices communicating directly between them without the need of third party relay devices like access points or routers. The D2D communication can also be for human to human communication e.g. two people talking on Skype™ with their mobile phones over WiFi, and/or for machine to machine communication e.g. Mobile phone and BT capable headset over BT. The most popular technologies used in the D2D networks nowadays are the BT and the WiFi [3].

B. Proximate Discovery

Proximate discovery, which is a quite new concept for end users in mobile networks, the ability for a device to passively and continuously search for relevant data or value in one's physical proximity or we can say ambience. Including but not limited to social media, proximate discovery is a platform fundamental in defining the next generation of services across an extensive set of use cases from advertising to Internet of Things (IoT). In a determined but moving area, it will connect people,

Copyright to IJARCCE

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319 5940
International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 5, Issue 7, July 2016

objects (including even animals), government and business [7].

C. Conventional Systems

The so-called conventional technologies which are very popular in this aspect are WiFi (or WiFi Direct), BT (including low energy LE) and global positioning system (GPS). Partially, we may include ZigBee and NFC too. Even though it is a very new technology, some features of NFC will be covered by LTE Direct (see section 3).

The conventional approach in proximate discovery and localization, Over-the-Top (OTT), is a cloud based database search mechanism which uses locale information of the device and searches for a pattern match in a list of places, most likely by using GPS.

In P2P communications, it is based on pairing multiple devices (usually not much than tens) and transmitting data using WiFi or BT.

D. Security in Conventional Systems

The security on conventional systems is based on the request password (or PIN in BT) architecture where the users have to manually provide the valid passphrase to authenticate their device to the network. In our research we did not see the security architecture of ZigBee, or other personal area (PAN) and body area (BAN) networks as rivals or competitors of LTE Direct security. Since they were mostly for lightweight devices like sensors and actuators instead of more complex computers like smartphones and tablets. Plus, ZigBee security represents a simpler model of the WiFi security with some modifications to make it work flawlessly in constrained devices [8], except for the multi-hop communication schemes. However, this is also not the main communication setting in LTE Direct and could be addressed in the application layer when necessary.

Specifically, BT provides link-level authentication with the use of a PIN which makes the devices to be paired. The alternative is to have a pre stored link key on each device to make this matching upon request [1].

In WiFi Direct, secure connection between peers is very similar to regular AP based WiFi connection. There are two possible security vulnerabilities in WiFi Direct; Wireless DoS and key cracking [9]. As an example, air sniffing and de-authentication attacks easily terminate a connection. But, use of WPA2 PSK makes key cracking very hard with the use of complex passwords, since the only known attack is dictionary attack.

E. LTE Direct

LTE Direct is a fairly new technology that proposes a device-to-device networking possibility for handheld devices over licensed radio spectrum. It is announced in 2011, standardized in 2013 and has been tested since then. Lately, commercial products are ready to be released supporting LTE Direct and the Software Developer Kit (SDK) has already be released by Qualcomm.

It provides devices a range of around 500 meters, thus, it can build up a D2D network of hundreds of devices in a relatively isolated geographical area. There are three main aspects that LTE Direct focuses on. Namely energy efficiency, connection security and proximity based services. Proximity services include identification, push messaging and transactions. File sharing is not its main purpose but it might be possible for small file sizes. It merges the OTT and P2P features of conventional systems in one body. Last but not least, the use of licensed radio spectrum that are solely "hired" to operators make the communication medium also isolated like the geographical area, which boosts the security by authorizing independently the communicating parties as seen in Fig. 1.

Device discovery in the range is made using periodical broadcasting and sniffing of, tiny, 54-bit or 128-bit data beacons, called "expressions", which contain device IDs and LTE Direct services supported by communicating devices. Hence, the device discovery becomes continuous and autonomous (as long as user has activated it), without severely affecting the device's' battery life unlike other proximity based solutions such as OTT based those utilize GPS, or BT-LE or WiFi Direct [4]. Hence, this process consumes much less energy when compared to conventional methods especially in long term and it can work flawlessly while other resource consuming applications are running on the background.

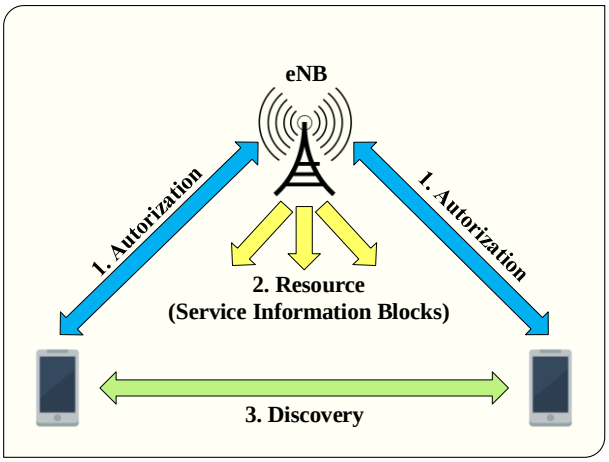

Fig. 1 Role of an operator in LTE Direct communication

F. Security in LTE and LTE Direct

The security architecture used in the LTE Direct is inherited by the overall project called LTE Advanced [3] which is an extension of the LTE/EPS mobile networks architecture [10].

1) LTE: The basic units in the LTE architecture is the E-UTRAN and the IP based backend protocol called Evolved Packet Core (EPC) [10]. The EPS/LTE architecture is fully compatible with the previous versions of the well-known mobile standards, 3G (UMTS) and 2G (GSM), but its basic infrastructure is based on Internet Protocol (IP), the EPC.

The key concept of the User Equipment (UE) having a Universal Integrated Circuit Card (UICC - a.k.a SIM Card

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319 5940
International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 5, Issue 7, July 2016

in predecessor systems) to perform the identification process with a shared key algorithm and the operators' backend with the evolved Node Base (eNB) participating in the UICC - eNB user identification in present and enhanced in the synergy between services and security. In the LTE/EPS the protocol between those two entities is not standardized and every operator can use its own due to the ownership of both part of the authentication process UICC and eNB. The protocol used behind the eNB to the operator's backend and main system is the IPsec [11].

The overall architecture ensures the confidentiality of the user and the device with the use of IMEI in the device part and the UICC subscription in the user part. The Authentication of the user is another important aspect in the LTE/EPS system but it is addressed similarly with the use of UICC and the authentication algorithms, Authentication and Key Agreement (AKA) in the eNB [10].

The LTE/EPS Architecture is versatile enough to support interoperability in security level between global standardized network technologies, apart from the defined by 3GPP, like WiMAX. This is done homogeneous by using authentication and security procedures defined in IKEv2 [12] and IPsec ESP [11]. This architecture design can provide potential use outside of the mobile industry as we describe later in the paper.

2) LTE Direct: The basic units in the LTE architecture is the E- UTRAN and the IP based backend protocol called Evolved Packet Core (EPC) [10]. The EPS/LTE architecture is fully compatible with the previous versions of the well-known mobile standards, 3G (UMTS) and 2G (GSM), but its basic infrastructure is based on Internet Protocol (IP), the EPC. Until here, we have briefly introduced the most secure mobile network at the time of writing. But since it is a direct connection between devices without using operator infrastructure, it may be hard to understand how this architecture will be beneficial for our case.

In the point of view of LTE Direct; that stationary security infrastructure and the UICC (or ME) of the users can be used to provide security in P2P connections, in terms of authentication and authorization see figure 1. Since the eNBs and the system behind the eNBs are not reachable by intruders - It is even not possible to use fake base stations in LTE unlike legacy GSM - operator infrastructure here provides a suitable secure channel to share keys and can be used to authenticate direct connection users by using their UICC and/or device IDs (IMEI, IMSI, TMSI, MAC etc) [10]. In WiFi and BT, there is no such secure channel to share keys, the only way is physical communication between peers. Moreover, in WiFi networks, it is possible to manipulate data packets and give wrong information to other peers (i.e. changing MAC address). But the use of operator infrastructure prevents malicious manipulations on transmitted data.

III.ANALYSIS

With the introduction of the LTE and the available bandwidth it provided, discussions have started in ways to utilize the LTE infrastructure and security to applications outside the usual mobile industry. The LTE Direct can be used to replace the conventional technologies, namely WiFi and BT mainly, exist now in a more convenient and secure for the user and the services that can use it. The security features of the LTE Direct give an advantage over the existed technologies in mainly 2 ways.

The first advantage is the authentication of the user securely enough via the infrastructure inherited by the LTE architecture with the potential use of UICC card. This way the user would not be prompted to enter a password for the authentication but automatically can be authenticated using the UICC of the operator. This authentication process requires minimal to non-user interference which let the users unobstructed from their original task because they do not need to interrupt their task to enter the password.

The second advantage that the LTE Direct has over the today used technologies is the security provided by the algorithms used in the industry which are more secure that the WEP [13] and WPA [9] of the WiFi. The security provided by the BT is adequate enough in the last BT-EDR edition via the E0/safer+ algorithm but the range of the BT availability is limited to 30m [14].
Though, we believe that the advantages above can be significant for the proposed use case; we are going to describe in the later part of this paper.

A. Possible Use Cases

For conventional methods, vendor profitability is quite enough to promote a new technology or standard. But here, operator profitability is another point. So, possible use cases should be analysed much more scrutinized. Because LTE Direct uses licensed band which is rented by mobile operators.

First question can be: "Why do we need another architecture, instead of the current technologies?". So, the boom in location based services including social media and gaming, moreover Internet of Things concept are two very important facts to take into account as well as mobile device abilities, which are constantly being improved.

A decade ago, people were not into share their personal information like their locations. But, nowadays they intentionally do that. Foursquare and Facebook are two huge arenas as good examples of where users can share their locations. Or TripAdvisor and Booking.com can be counted as promotion and suggestion platforms again based on locations. One big problem in these services is wrong locale information or duplicate entry for the existing places (such as cafés or hotels). Here, even though it is not accurate as GPS, LTE Direct offers a more

Copyright to IJARCCE
DOI 10.17148/IJARCCE.2016.5779

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319 5940
International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 5, Issue 7, July 2016

reliable solution while it will be "always on". On the other hand, they are good places to advertise. LTE Direct would move that opportunity one step ahead, by enabling multicasting of advertisements directly from shops to the people around. Moreover, persona specific offers and digital coupons can be transmitted to devices around. This brings a new approach to "happy hours" and customer loyalty rewards.

D2D push messages can be used in emergency cases too. They will not just have used to inform people around an emergency situation, plus people around will be able to provide more information to other people and institutions. For example, a fire or an accident. In the accident case, or when there is a construction, people and drivers would be informed about that.

Another huge arena/market: Online gaming. First revolution was broadband internet and second revolution is mobile broadband, supported by powerful mobile equipment. BT is the dominating system to connect peers or devices like controllers; while WiFi Direct is recently emerging. But, LTE Direct offers a total new experience with ~500 m range (in LOS case) and anonym connections without a peer limit (i.e. most WiFi b/g APs accept 32 peers). Sharing the same "game world" (for readers who are not familiar with gaming slang, basically game screen) or even hunting for virtual objects (usually called items) in the real world would be possible in quest style games. This will create a new arena for game developers.

Mobile payment systems, including mobile digital signatures, are currently under development and even though some trials are deployed, a widespread usage couldn't be achieved yet. Extensive use of LTE Direct in a diversity of MEs (incl. phones, tablets, POS devices, cash registers etc.) would provide a revolutionary and very easy way to pay the bills and checks shops, especially in cafés and restaurants. Cashier could send the bill as a push message using LTE Direct and the customer could pay it in where he/she is. The bill could be reflected to operator's monthly bills. Same applies to toll booths, theatres, funfairs etc. These kind of methods of course requires software support and security at application level should be provided. Currently NFC is used as a mobile payment system, but since NFC has a range of 5-10 cm for "contactless payments" (practically means still touching) [15], it just replaces money and cards, while LTE Direct would offer much more options, including the coupons mentioned above.

LTE Direct may also bring new opportunities to Internet of Things and object tracking. As an example, tracking untied pets (via an LTE Direct enabled collar) in an urban environment, or keeping a virtual eye on the cars in the parking lot can be very easy using LTE Direct. First, it natively supports IPv6, which is a required standard for IoT, while conventional systems would require "updates". Second, coverage range of ~500 m is larger than BT and WiFi, plus it can work indoor environment reliable unlike GPS. Third, a relay mode will be available to transfer data from sensor networks to stations. Last but not least, a handover from direct (P2P) mode to operator infrastructure mode is possible, when peers are moving and getting out of their ranges. This feature provides an uninterrupted communication between devices on the move.

Fig. 2 below, shows an example communication frame between a mobile user and a fixed station in an LTE Direct enabled ecosystem. Here, a walking person, a customer, a vehicle or any other moving object with an LTE Direct enabled device that is continuously connected to their operator and runs LTE Direct (in idle mode) approaches to the proximity (range) of another fixed LTE Direct enabled device, which can be a payment station or a check point, and automatically pairs after discovery with beacons.

Alternatively, LTE Direct mode could initially be turned off and when the mobile user approaches approximately around the range of the fixed station, the provider's eNB could trigger the activation of LTE Direct mode and by this way extra energy efficiency can be provided. When devices are in range, any operation like messaging, shopping transactions or log tracking is made while mobile user is still moving. Then mobile user leaves the area and the communication terminates. LTE Direct could switch to the idle mode, or as explained in the alternative method, it can be forced to turn off via eNB. In addition to the proximity aware triggering, eNB here can establish a secure indirect channel between directly communicating devices to allow them to share sensitive information like security keys. No need to mention that these are not possible with conventional systems.

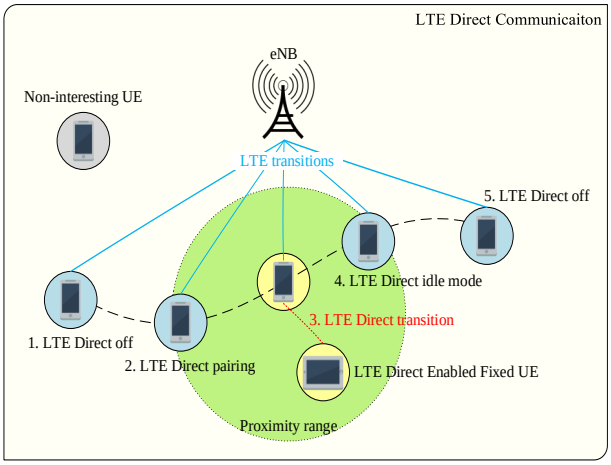

Fig 2 Communication between a mobile user and a fixed station

B. Pros and Cons

The LTE Direct technology has significant advantages over the conventional technologies. The security features of the LTE Direct is far more advanced that of the WiFi especially, it provides stronger authentication encryption.

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319 5940
International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 5, Issue 7, July 2016

The longer range of the LTE Direct and the greater capacity for simultaneous connections in the same area gives a potential availability where the other technologies already in use would have failed. The competing BT fails to have a range more than a few tens of meters while the latest 802.11n WiFi promises range around 50 meters but very limited simultaneous connections [14]. Apparently, the most significant benefit would be the energy efficiency of LTE Direct, since in the discovery enabled idle mode, when no specific application is running, LTE Direct consumes up to 120 times less energy than WiFi Direct, while in the same period of time LTE Direct discovers up to 20 times more devices around [16].

On the other hand, we see some (mostly temporal) disadvantages. First of all, while device-level market penetration for WiFi and BT are extremely high, almost all mobile equipment even the low end ones contain WiFi chips. So that, cumulatively 5 billion WiFi enabled devices are shipped as of 2012 [17], same applies to BT too. Contrarily, although it is being very popular, at the time of writing, LTE is not that widespread. Many countries don't have LTE infrastructure and many of them making trials yet [18]. Another problem could be the funding of the licensed band. Unlike WiFi and BT which use ISM bands, users of this system should pay for the frequency occupation (usually 2600 MHz bands but depends on the country). But at least, it doesn't have to be the end user. Sponsor or advertiser companies can do that instead of end users.

C. Security Threats

LTE Direct brings a totally new aspect to D2D security, when compared to conventional methods, WiFi and BT. But in the meantime it may enable new threats by the emerge of new applications. All security threats in mobile networks can be found elsewhere [10]. Specifically, in this type of a network, malicious actions may affect Availability (by DoS or DDoS attacks), Authorized access (by ID spoofing) and Confidentiality (by Man-in-the-Middle or Replay attacks) of network [6].

When operator signal is available, LTE Direct can use that common infrastructure to protect confidentiality of the data by using key distribution ability of the E-UTRAN and intensive encryption and integrity systems like 128-EEA2 and 128-EIA2, which use AES [19]. It is basically the EPS AKA procedure. Additionally, IPSec is used in operators' network and it is not possible to add malicious eNBs to the system. Even though operator support is not available, system will be as secure as WiFi, because LTE (incl. LTE Direct) is an all-IP network unlike legacy GSM and 3G (UMTS). Furthermore, multi-layered ID information, which consist of IMEI, IMSI, TMSI, Subscriber Number (Phone No.), MAC Address and IPv6 support can make authorized access much reliable. This also prevents ID spoofing. As can be seen here, with the help of the application layer, LTE Direct is not vulnerable to unauthorized access and data disclosure.

Availability protection, which is under research for a long time, is a big problem in all kind of wireless networks, as well as LTE Direct. Because of the proximate discovery based nature, Signal Hiding techniques are not useful for LTE Direct [20]. Very wide bandwidth of LTE-A invalidates famous Denial-of-Service (DoS) attacks, but one should not forget that we are talking about a crowded environment and a "super" multi-user network. Though, Distributed- Denial-of-Service (DDoS) attacks still can interrupt the connection between peers [21]. In that case with help identification techniques, intruders can be detected and discarded, for example, at IP level. This area needs to be researched more. And there is nothing to do to jammers, that quashes radio signals.

IV. CONCLUSION

In the days to come, the discussions about the use of a different architecture for D2D network will flame and mobile and communication industry will turn a solid eye on LTE Direct. The conventional technologies are dominant today and the possibility to see the LTE Direct be adopted by more vendors and company looks difficult but its architectural advantages which provide a secure and multiuser environment in a local area and the minimal user interaction for the authentication and use of the network makes this emerging technology a very strong candidate to pick for an alternative in D2D networking [10]. The wide variety of possible location and context aware applications of LTE as well as the "always on" feature could eventually become from Qualcomm's study item call, to work item and finally an established technology. The only major drawback at the time of writing this paper is that this technology has low level of device adaptability and is parent technology LTE is not yet implemented in a lot of countries [18]. These issues would surely could be proven minor regarding the advantages of this new architecture that we can see that it has major potentials in being adopted among operators and vendors. As final words; we've found LTE Direct a secure, reliable, flexible and energy- efficient way to communicate in mobile ad-hoc networks, that should be researched and improved a little more.

From now on researches may follow two points of view: business case and technical case. In the business case, LTE penetration, cost/revenue streams and bandwidth allocation should be researched. In the technical case, we need more performance tests on the field to determine in which exact applications we should leave conventional systems, plus increasing availability protection by taking advantage of ad- hoc networking, additionally impact of widespread usage of femtocells can be researched.

ACKNOWLEDGMENT

We would like to acknowledge Rune Hylsberg Jacobsen at Aarhus University for his valuable technical support and contribution to this study.

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319 5940
International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 5, Issue 7, July 2016

REFERENCES

[1] T. Muller. (1999) Bluetooth Security Architecture. [Online]. Available:http://www.bluetooth.org/docman/handlers/DownloadDoc.ashx?doc_id=90&vId=129
[2] Telecommunications and information exchange between systems - Local and metropolitan area networks - Specific Requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specs. Amendment 10: Mesh Networking, IEEE Std 802.11s-2011, 2011.
[3] L. Lei, Z. Zhong, C. Lin, and X. S. Shen, "Operator Controlled Device-to-Device Communications in LTE Advanced Networks," IEEE Wireless Communications, vol. 19 (3), pp. 96 – 104, June 2012.
[4] LTE Direct Workshop, White Paper, Qualcomm, 2013.
[5] D. Williams, G. Tsirtsis, and R. Hovey. "Text proposal for the scope of LTE-Direct study item TR 22.###," 3GPP TSG-SA WG1 Meeting #55, August 2011.
[6] S. Ramasubramanian, S. Chung, S. Ryu, and L. Ding, "Secure and Smart Media Sharing Based on a Novel Mobile Device-to-Device Communication Framework with Security and Procedures," in Proc. RIIT '15, 2015, pp. 35-40.
[7] LTE Direct Overview: The Case for Device-to-Device Proximate Discovery, White Paper, Qualcomm Research, 2013.
[8] Low Power RF Solutions - ZigBee Security, Texas Instruments [Online]. Available: http://processors.wiki.ti.com/images/7/7b/10_-_ZigBee_Security.pdf
[9] S. Yoon, S. Park, H. Park, and H. S. Yoo, "Security Analysis of Vulnerable Wi-Fi Direct," in Proc. ICCNT'12, 2012, pp. 340 – 343.
[10] D. Forsberg, G. Horn, W. D. Moeller, and V. Niemi, LTE Security, 2nd ed., Wiley, 2012.
[11] IP Encapsulating Security Payload, [Online]. Available: http://tools.ietf.org/html/rfc4303, IETF, 2005.
[12] Internet Key Exchange Protocol Version 2 (IKEv2), [Online]. Available: tools.ietf.org/html/rfc5996, IETF, 2010.
[13] N. Cam-Winget, R. Housley, D. Wagner, and J. Walker, "Security flaws in 802.11 data link protocols," Communications of the ACM, vol. 46 (5), pp. 35 – 39¸ May 2003.
[14] J. Padgette, K. Scarfone, and L. Chen, Guide to Bluetooth Security, [Online]. Available: csrc.nist.gov/publications/nistpubs/800-121-rev1/sp800-121_rev1.pdf, Nist US department, June 2012.
[15] Near Field Communication, White Paper, Nokia, 2007.
[16] LTE Direct Trial, White Paper, Qualcomm, Feb 2015.
[17] Wireless Spectrum, Services, and Technology Deployment Tracker, ABI Research, December 2012.
[18] 274 LTE Networks Commercially launched in 101 Countries, Map, GSA, February 2014.
[19] LTE and the Evolution to 4G Wireless: Design and Measurement Challenges, White Paper, Agilent Technologies, 2008.
[20] M. Choi, R. J. Robles, C. Hong, and T. Kim, "Wireless Network Security: Vulnerabilities, Threats and Countermeasures," International Journal of Multimedia and Ubiquitous Engineering, vol. 3 (3), pp. 77 – 86, July 2008.
[21] R. P. Jover, "Security Attacks Against the Availability of LTE Mobility Networks: Overview and Research Directions" in Proc. WPMC'13, 2013, pp. 1 – 9.