# Secure D2D Communication in 5G Networks

R.Yadav, S.Sanyal, Member IAENG

***Abstract*- 5G technology is presently the most prominent technologies in network domain. Although, it is said to be available by year 2020, but still there are lot of views about the features and benefits which 5G will offer to the world in comparison with 4G.Also there are lot of discussions about its resource requirements with which our world will enter into a new era of mobile technology after implementing these requirements. With the concept of Internet of Things brought together by 5G, we can expect that this technology will go one step ahead as future network technology. As different application areas as well as new architecture and technologies will grow with 5G, so we can also expect that we will face different security and privacy protection challenges. One of the most promising area of 5G technology is device to device communication. With the growth of such promising technology, we know that since 2G, user privacy and security has been a very important issue. In this paper, we broadly review D2D communication security in 5G networks. At last, future research directions are presented which can strengthen the security of 5G technology.**

***Index Terms*— D2D, MITM, 5G.**

## I. INTRODUCTION

5G technology in the near future will replace existing 4G technology in many nations of the world. Software-defined networking (SDN) and virtualization which are latest developments in wireless technologies are the main areas which serves as the base for next generation 5G technology. Because of having high bit rates with even more than 10gbps and low latency, as an upcoming technology, 5G will be highly useful in Internet of Things (IoT) as well as other applications. We will have a full-fledged connected mobile society through 5G by designing various network services such as mobile fog computing [1], smart grid technology [2], car-to-car connectivity and block chain based services. In the upcoming mobile technology era, 5G systems are an advanced step. Being an important part of network society, these systems should not focus on voice and data functionality which we presently have, but these should also provide support for new areas of application as well as large number of devices so that we can have a completely connected mobile society. In comparison with the existing connectivity technologies, 5G is considered more complex. In order to being known as real world wide wireless web, our world is continuously making a big growth and is going to join the upcoming 5G connectivity era. In such a big 5G network domain area, a big amount of financial, electronic media, medical records, and customer files which may be a confidential data will be transmitted throughout the world via wireless channels. So we can expect 5G design to possess an unrivalled security service as the top priority for safe transmission of such confidential data. After 4G, 5G is the next level of mobile communication technology.5G technology when compared with existing 4G will have system capacity of 1000 time along with 10 time spectral efficiency 25 times cell throughput, 10 Gbps as peak data rate in case of low mobility and 1Gbps for high mobility.

In this paper, we will review 5G technology vision, its key terms, protocol stack along with specifications and differences between 4G, 5G and majorly focusing upon D2D communication in 5G with future research directions.5G as an upcoming technology has been briefly introduced in section 2 with the four layer protocol stack which is explained in detail with various layer functionalities along with technical specification. Section 3 illustrates the technical differences between 4G and 5G technology in consideration with security related issues.D2D communication in 5G has been discussed in section 4 with four D2D design models on which 5G technology is based. Various security related issues which happen in D2D communication has been explained in section 5 and at last section 6 shows a detailed literature survey along with future research directions for strengthening D2D security in 5G technology

## II. OVERVIEW OF 5G TECHNOLOGY

Next generation mobile world will have below mentioned features under the umbrella of 5G technology [3]:

- 5G will introduce a real world wide wireless web in which there will be no restrictions or boundaries towards access and zone issue.
- Multimedia newspaper and TV programs will have HD clarity capability.
- As compared to existing mobile generations, there will be much more speed of data transmission.

Mr. Rajesh Yadav is Assistant Professor in Department of Computer Science in School of Engineering and Technology at BML Munjal University, Gurgaon, India. He is B.E. and M.Tech., PhD. (P) in Computer Science and Engineering. His research area is Wireless Networks and 5G.
Email: rajesh.yadav@bmu.edu.in
Dr. Sudip Sanyal is the Director-Faculty of CSE, School of Engineering Technology. He has 32 years of teaching experience in leading Universities like IIIT, Allahabad, Banaras Hindu University & University of Roorkee.
Email: Sudip.sanyal@bmu.edu.in

ISBN: 978-988-14047-9-4
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

- Wearable devices will have Artificial Intelligence functionalities.
- Internet protocol version 6 (IPv6) functionality with a feature of assigning mobile IP address depending on connected network as well as location.
- There will be one unified global standard.
- Ubiquitous computing because of pervasive networks, as a result of which network users will have the flexibility of freely moving b/w various access technologies such as 2.5G, Wi-Fi, PAN as well as any other access technology of future. In addition to this, 5G technology can also be enhanced to provide multiple number of simultaneous data transfer paths.
- Cognitive radio which is known as smart radio technology is one of the best feature of 5G, through which various radio technologies can have efficient same spectrum sharing by adaptively using the unused spectrum as well as adapting the transmission scheme in accordance with the technologies currently sharing the spectrum.

5G technology is assumed to possess different requirements like user confidentiality, device identity, signaling data confidentiality as well as platform security requirements [4].

Moreover, 4G technology has given an experience to users in special network scenarios such as connectivity in high speed train with vehicle speed with communication up to 250km/hr. On the other hand, 5G networks will be capable of doing the same even when the train reaches a speed of 350 to 500km/hr.[5].Figure 1 shows 5G network [27].

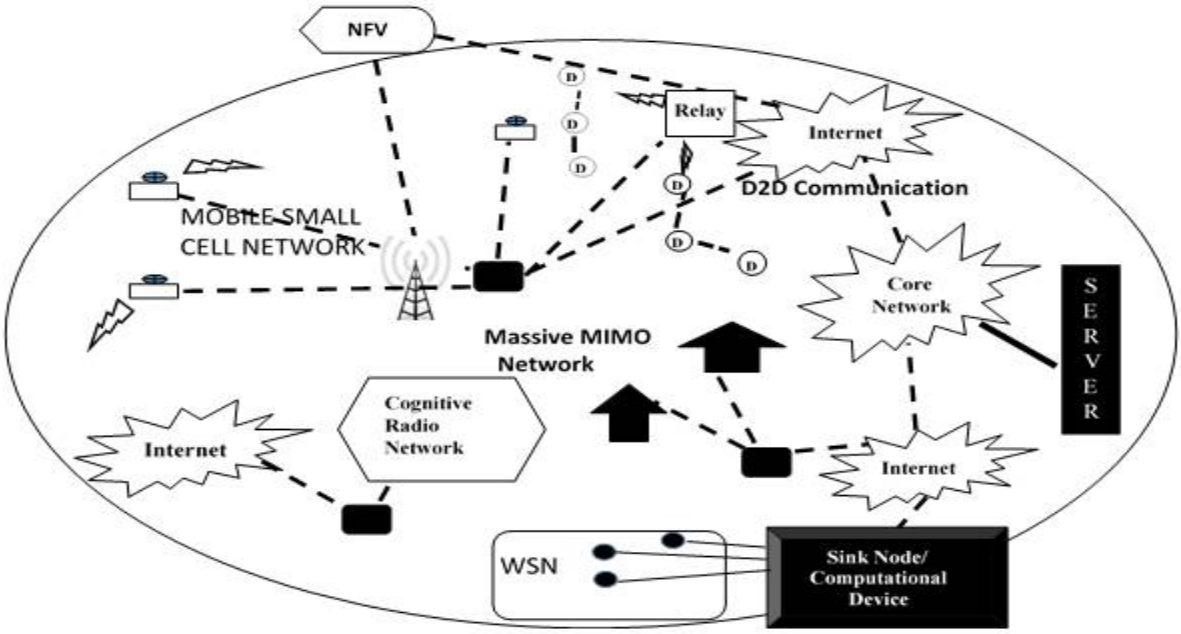


Fig.1. 5G network architecture

*A. 5G Protocol Stacks*

The protocol stack of 5G is designed with having four layers as shown in Figure 2[11].

| | |
|---|---|
| **Application Layer** | **Application (Services)** |
| **Presentation Layer** | |
| **Session Layer** | **Open Transport Protocol (OTP)** |
| **Transport Layer** | |
| **Network Layer** | **Upper Network Layer** |
| | **Lower Network Layer** |
| **Data Link Layer(MAC)** | **Open Wireless Architecture (OWA)** |
| **Physical Layer** | |

Fig. 2. 5G Protocol Stack

*Physical/MAC layers*

In the near future with 5G mobile network, we will have communication model systems like cellular, wireless local area network systems, wireless connectivity of short range, broadband wireless systems as well as wired system type of different access technologies will be brought together on one single platform to cater the needs of various service requirements in addition to radio environments. It is called open wireless architecture (OWA) [10].As shown in figure 2, layer 1 & 2 i.e. physical and medium access control layers are part of this architecture.

*Network layer*

This layer is composed of two layers i.e. upper network layer & lower network layer. 5G devices should maintain a virtual multi-wireless network, due to this reason, this layer is distributed into 2 layers i.e. the lower network layer which is used for each interface and for mobile devices, the upper network layer is used. The middleware part between the upper & lower layer will perform the translation of address from upper network address (IPv6) to various lower network IP addresses (IPv4 or IPv6) [11].

*Open Transport Protocol (OTA) layer*

As we are aware that mobile and wireless networks are considered different from point of view of transport layer. In all TCP

ISBN: 978-988-14047-9-4
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

versions, lost segments problem happen due to the reason of network congestion, on the other hand high bit ratio in the radio interface is the reason for same in wireless scenario. Therefore, it is required to implement some changes for mobile and wireless networks so that lost or damaged TCP segments can be retransmitted. Depending on the base station wireless technology, mobile devices in 5G technology can have the transport layer (TCP, RTP etc.) by downloading and installing it. It is known as Open Transport Protocol (OTP) [11].

*Application layer*

Providing good service quality along with required data format as well as data encryption/decryption is responsibility of this layer. Moreover at this level, best connection will be selected for a given service.

*B. 5G technology specifications*

High throughput feature along with using existing communication technologies like 2G, 3G and 4G, upcoming 5G technology will possess technical specifications as mentioned in table 1[12]:

TABLE 1
5G SPECIFICATIONS

| Specification | 5G Support |
|---|---|
| Bandwidth | 1Gbps or higher |
| Frequency | 3 to 300 GHz |
| Access technologies | CDMA/BDMA |
| Technologies | Unified IP, seamless integration of broadband, LAN/PAN/WAN/WLAN and 5G based technologies |
| Applications/Services | Wearable devices, dynamic information access, HD streaming, smooth global roaming |
| Core network | Flat IP network, 5G network interfacing (5G-NI) |
| Handoff | Vertical, Horizontal |
| Peak Data Rate | Approx. 10 Gbps |
| Cell Edge Data Rate | 100 Mbps |
| Latency | less than 1 ms |

## III. 5G vs 4G IN TERMS OF SECURITY AND PRIVACY

Security issues of 4G and 5G networks are compared by going through the security issues faced by 4G networks followed by the security issues which can come in the next generation 5G technology.

*A. 4G Security Issues*

*Scrambling attack*

This kind of attack happens for small intervals of time. Specific frames are attacked in case of 4G networks. In order to disrupt the service, the user management/ control information is attacked by the attacker.

*Interference*

LTE and WiMAX which are 4G technologies have been found vulnerable to interference problems.

*Signal Jamming*

Because of high capacity and system enhancements, LTE and WiMAX, which are 4G technologies face signal jamming attacks. Moreover, by capturing the unsafe messages broadcasted from base station known as eNodeB, the physical resource blocks are identified by low-power smart jamming attacks.

*Location tracking issues*

In whole of the location area, paging messages are delivered, as a result, even in a high range, the attacker can easily identify the subscriber location [2].Also, using smart paging process, even within small area of LTE cell size, the location of subscriber can be found by the attacker.

In addition to the above mentioned security issues which happen in 4G networks, denial of service issue is also faced by the networks along with open nature, in which from many external connections, through peer operators, infrastructure of 4G can be accessed thereby making 4G network vulnerable to security problems. Also if we observe that, as many service providers share the core network infrastructure, so the entire infrastructure can be affected if one of the service provider security is compromised.

*B. 5G Security Issues*

5G technology is going to be built around a model of networks of networks. Existing 4G security techniques will be enhanced so as to cater the needs of 5G technology, even then the security requirements of 5G is much more as compared to 4G as well as other existing generations. The attack surface will grow with the arrival of 5G in world and as a result many security issues will come into picture.

*Network slicing security Issues*

According to the services required in future, the network will be sliced as per the design of 5G technology. Moreover configuration of every slice will be done according to mandatory requirements, such as for IOT devices, around ten percent of network resources can be reserved. There will also be some security issues due to network slicing like different policies as well as various security protocols in different slices along with other issues like denial of service for other network slices, side channel attacks across slices, impersonation attack.

*Data manipulation*

Because of shifting towards NFV, various security issue will be faced by 5G technology i.e. dedicated hardware will be replaced by virtual machines in case of mobile networks for cost minimization and to speed up the new services. Because of happening of all this, there are good chances of data being modified thereby making 5G environment more challenging because of security problems.

*Equipment cloning*

It is also an important issue in 5G technology, which if occurs can be a reason of attack leading to network overloading and then making denial of service to happen in network. For avoiding this problem, device identity management & authentication has to be performed strongly for ensuring good network security.

*Rogue devices*

Any attacker can pretend to be a real device and therefore can manage to join the communication scenario, as a result sensitive information can be accessed by a rogue device.

*Denial Of Service*

In 5G network, a large number of devices will be a part of communication scenario, so it is possible that they can face denial of service issue which can further lead to severe consequences.

ISBN: 978-988-14047-9-4
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

*Eavesdropping*

In case of 5G technology, there will be multiple number if devices communicating with each other, so as in case of device to device communication environment, an eavesdropper will be able to access communication line without having sender & receiver aware of it. So, the encryption techniques should be designed in such a form that eavesdropper cannot open the transmitted message and the communication progresses safely.

*Man-In-The-Middle attacks*

MITM can lead to a security problem in case of 5G technology, in which case the attacker can affect data integrity as well as confidentiality and making it less secure. This all happens when the communication line is eavesdropped by the attacker thereby putting an impact on data integrity using interception and modification of message.

## IV. DEVICE TO DEVICE COMMUNICATION IN 5G NETWORKS

D2D is a very important technology having different devices capable of participating in direct communication with one another without having base station type of bigger entities involved. With 5G technology, device to device communication concept will surely see a big growth, as it will be possible for nearby devices to look for each other and then will proceed to directly communicating with each other. This will take our world to the next step where communication capability will grow in addition to dealing with other important parameters like power consumption and delay. After seeing a full fledge growth of 4G technology, the whole world is looking forward towards upcoming 5G technology which will possess lot of previously mentioned features along with D2D communication technology playing a very important part in it[23].Two tier network of 5G is composed of macro cell tier & device tier. The base station and device communicate with each other in macro cell tier scenario similar to a conventional cellular network where as in case of device tier scenario, devices communicate with each other. In addition to this, the network traffic can be relayed by a device for assisting other devices, the base station of course participates in this communication process.5G technology will have 4 different device tier communication models [24].

*A Device relaying with operator controlled link establishment (DR-OC)*

In this scenario, it is still possible for a device to communicate with base station even when it is in poor cell coverage area. It happens by relaying the data via other network devices in the network. DR-OC is shown in figure 3.

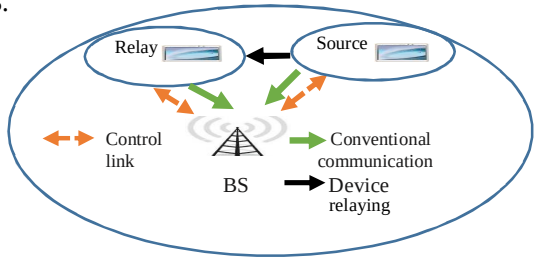


Fig. 3. Device relaying with operator controlled link establishment (DR-OC)

*B Direct D2D communication with operator controlled link establishment (DC-OC)*

As we can see in figure 4, after the operator establishes a link between the source and destination device, these devices can communicate with one another without having any role of base station between them.

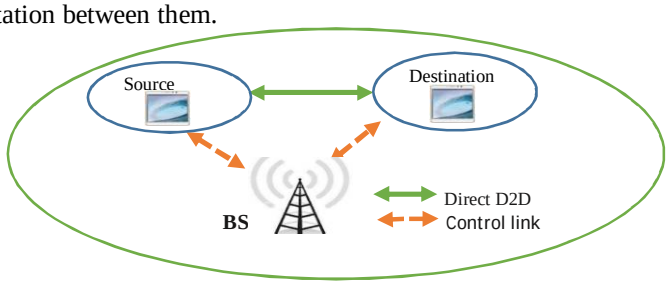


Fig.4. D2D direct communication with operator controlled link establishment (DC-OC)

*C Device relaying with device controlled link establishment (DR-DC)*

In this scenario as illustrated in figure 5, both the devices i.e. source & destination can communicate with each other by relaying the transmission between each other. Also, the operator does not perform any link establishment role in it.

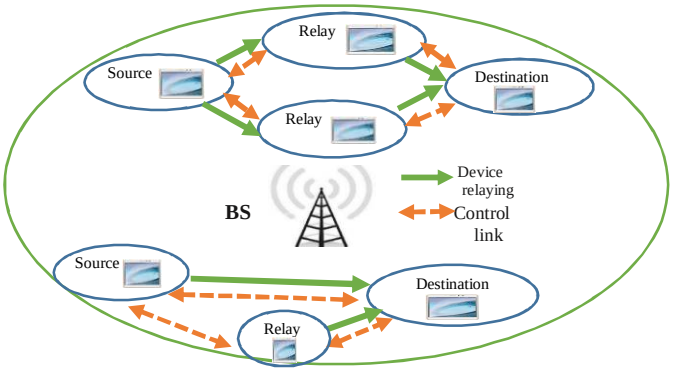


Fig. 5. Device relaying communication with device controlled link establishment (DR-DC).

*D Direct D2D communication with device controlled link establishment (DC-DC)*

This design model is based on direct communication b/w source device & destination device without any relaying mechanism and operator control process as depicted in figure 6.

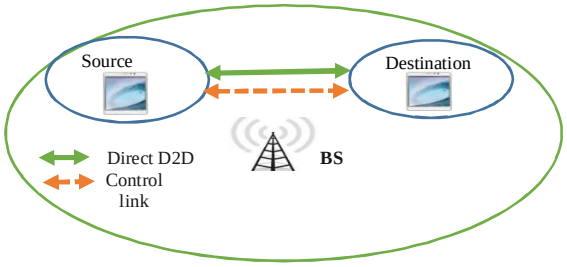


Fig.6. Direct D2D communication with device controlled link establishment (DC-DC).

## V. SECURITY IN D2D COMMUNICATION IN 5G NETWORKS

There are many security challenges faces by 5G networks which should be handled carefully and by overcoming all these challenges, D2D communication can become a

ISBN: 978-988-14047-9-4
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

prominent technology for 5G networks. Since other devices also play role in routing of data in D2D, therefore for ensuring privacy, security has to be maintained strongly. MITM is considered a very crucial attack and therefore it should be handled carefully to make D2D communication safer. As shown in figure 4 illustrating DC-OC model, since the communication also involves base station, so the relaying devices can be authenticated by it and using proper encryption techniques, devices can have ensured transmission privacy. On the other hand, if we see other 2 design models i.e. DR-DC & DC-DC, we see that communication happens between devices without any base station or server control. As we are aware that the devices have to discover each other in addition to the adjacent relays also before the start of communication, while doing so, identity information of devices is broadcasted so as to inform other devices about their presence and based on this, the devices can go for either direct device to device communication or device relaying process [8].It can be understood that such scenarios of communication are very challenging to be handled while dealing with security and privacy as the attacker can perform MITM attack during the communication process. MITM can be characterized by three ways i.e. based on impersonation techniques, communication channel in which the attack is executed and location of attacker as well as target in the network [9].

## VI. RELATED WORK DONE IN DEVICE TO DEVICE SECURITY

Wang et al. [13] proposed security architecture for D2D communication in which they discussed security requirements like Integrity, Confidentiality Non-Repudiation (NR) and privacy. In addition to this, they also suggested D2D communication research directions like key management, authentication scheme and access control methods.

Zhang et al. [14] suggested an architecture for 4G device to device communication and investigated various issues of privacy such as identity privacy, location privacy as well as data privacy. The authors proposed security solutions for both application as well as physical layer along with a framework for cross physical and application-layer security.

Sedidi et al. [15] suggested a novel key exchange protocol for 5G networks for network supported device to device communication. This protocol makes use of diffie hellman key exchange. There is less communication overhead as well as less computational time when compared to previously existing mechanisms.

Fang et al. [16] suggested 5G security architecture in the proposed work, an analysis has been done on flexible authentication and identity management. Also they surveyed handover procedure & presented future research direction for ensuring that 5G technology works safely for real life applications.

Haus et al. [17] investigated security and privacy in D2D communication. The authors considered various security and privacy challenges such as device discovery, network communication, proximity services as well as location privacy. Existing mechanisms are analyzed and new security and privacy issues are identified for further research.

Chen et al. [18] investigated downlink secure communication without CSI from device to device users as they are present in cell edge. In order to make communication safer, the base station uses a transmission technique based on artificial noise.

Ismaiel et al. [19] proposed a scalable MAC protocol and worked on point coordination function in D2D communication. The authors suggested a three tier architecture which can offload traffic in mobile network from macro cell to small cell basically in a dense environment. Network capacity is shown enhanced in the proposed method.

Malandrino et al. [20] discussed integrating I2D i.e. infrastructure-to-device (I2D) mode and device to device mode & then discussed about resource scheduling in heterogeneous networks b/w device to device.

Elrahman et al. [21] proposed a secure device to device group communication mechanism by using identity based encryption (IBE) technique. Inter domain as well as intra domain security is considered and ECC based group key communication scheme is used in the proposed method. In addition to this, it is also based on IBC weakness with group keys management designing method.

Asadi et al. [22] did literature survey on D2D communication in mobile networks. In band as well as out band were two D2D groups on which their survey is based. Underlay and overlay are the two D2D categories, in addition to this, out band D2D is further categorized into controlled and autonomous. Underlay D2D faces interference management & power control issues whereas these issues are not present in overlay type as we know that mobile and D2D resources have no overlapping b/w them. The authors surveyed weakness as well as strength in previous research work in the area of D2D and discussed its applications in real world.

Lee et al. [23] focused on confidentiality of data in case of 5G networks. Through physical layer security, better results can be obtained since there is no dependency on computation as well as complexity involved. Because the devices can join and leave the network at any time, therefore 5G networks should have end to end security just like in case of ad hoc scenario. Also, the authors made use of low power communication and receiver movement mechanisms so as to work efficiently against eavesdropping attack.

3GPP [24] presented an authentication method by making use of EPS AKA and then the key generated is delivered using the protocol instead of using device IMSI number.

Boccardi et al. [25] focused on 5G physical layer security along with cloud Ran framework. Eavesdropping issues are focused by the authors which can take place while devices communicate. The work proposed by authors will provide safety to devices by keeping them separate from devices which are untrusted and in addition to this, devices can send messages using various channels.

Yang et al. [26] presented work like network coding for ensuring safe device to device communication as well as offering physical layer security in order to secure communication from any attacks endangering data integrity & confidentially.

Elham [7] presented device to device communication in 5G networks. The author suggested some research direction pointing out that how research should be done in D2D communication field as it is a key technology for 5G real life

ISBN: 978-988-14047-9-4
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

applications.

Dubrova et al. [6] proposed an authentication mechanism based on CRC. The method can detect all double bit errors as compared to already existing methods. The proposed method can be used for safe authentication in 5G technology. 5G work on security architecture should be started to ensure that it has inbuilt security right from the start. Important steps will be how to make device to device communication in 5G non vulnerable to MITM type of attacks. Through this paper, we go one step forward in the direction after identifying D2D security issues and we hope that this work will be promoted towards a sound 5G security architecture.

## VII. CONCLUSION

5G technology is expected to connect the entire world without any limits, therefore it should possess unbelievable and extraordinary data capabilities along with other features. Through 5G, access to information will be universal and uninterrupted in the world, also communication as well as entertainment will open a new dimension to our lives thereby changing the lifestyle meaningfully. We can also expect 5G to face many challenges in terms of security and privacy with the increasing number of connected users. In this paper, we presented a detailed survey of how device to device communication needs a strong security design to overcome the privacy issues. Future research direction of 5G really needs to focus upon securing its connected devices from such attacks. We really need a strong mutual authentication mechanism to ensure that crucial attacks like man-in-the-middle can be avoided and the communication happens in a secure way between the devices.

## REFERENCES

[1] Mithun Mukherjee, Rakesh Matam,Lei Shu,Leandros Maglaras, Mohamed Amine Ferrag, Nikumani Choudhury, Vikas Kumar, "*Security and Privacy in Fog Computing: Challenges*", IEEE Access,2017.

[2] Mohamed Amine Ferrag, Leandros Maglaras, Ahmed Ahmim,"*Privacy-preserving schemes for ad hoc social networks: a survey*", IEEE Communications Surveys & Tutorials, 2017.

[3] Asvin Gohil, Hardik Modi, Hardik Modi,"*5G technology of mobile communication: A survey*", 2013 International Conference on Intelligent Systems and Signal Processing (ISSP), 2013.

[4] Gunther Horn, Peter Schneider, "*Towards 5G Security*", Trustcom/BigDataSE/ISPA, 2015 IEEE, August, 2015.

[5] Cheng Xiang Wang, Fourat Haider, Xiqi Gao ,Xiao Hu You, Yang Yang, Dongfeng Yuan,Hadi M. Aggoune,Harald Haas, Simon Fletcher,Erol Hepsaydir,"*Cellular Architecture and Key Technologies for 5G Wireless Communication Networks*", IEEE Communications Magazine,Vol. 52, Issue 2, February 2014.

[6] Elena Dubrova , Mats Näslund , Göran Selander,"*CRC-Based Message Authentication for 5G Mobile Technology*", Proceedings of the 2015 IEEE Trustcom/BigDataSE/ISPA, p.1186-1191, August 20-22, 2015

[7] Enayati, Elham,"*Device-to-Device Communication Technology under 5G Networks*", First International Conference on Internet of Things, Applications and Infrastructure (IoT2017), 2017.

[8] Gábor Fodor, Erik Dahlman, Gunnar Mildh, Stefan Parkvall, Norbert Reider, György Miklós, Zoltán Turányi,"*Design aspects of network assisted device-to-device communications*",IEEE Communications Magazine,2012.

[9] Aiqing Zhang, Jianxin Chen, Rose Qing Yang Hu, Yi Qian," *SeDS: Secure Data Sharing Strategy for D2D Communication in LTE-Advanced Networks*", IEEE Transactions On Vehicular Technology, Vol. 65, No. 4, April, 2016.

[10] Willie W. Lu, "*An Open Baseband Processing Architecture For Future Mobile Terminal Design*", IEEE Wireless Communications, Vol. 15, Issue 2, April 2008.

[11] "5G network architecture| and 5G protocol stack", http://www.rfwireless-world.com/Tutorials/5G-network-architecture .html, March,2018.

[12] Rehman Talukdar, Mridul Saikia,"*Evolution and Innovation in 5G Cellular Communication System and Beyond: A Study* ", arXiv: 1407.4335v1 [cs.NI] 16 Jul 2014.

[13] Mingjun Wang, Zheng Yan,"*Security in D2D Communications: A Review*", trustcom/BigDataSE/ISPA, IEEE, August, 2015.

[14] Aiqing Zhang, Xiaodong Lin,"*Security-Aware and Privacy-Preserving D2D Communications in 5G*", IEEE Network", July/August 2017.

[15] Ravindranath Sedidi, Abhinav Kumar, "*Key Exchange Protocols for Secure Device-to-Device (D2D) Communication in 5G*", Wireless Days (WD), March, 2016.

[16] Fang, Dongfeng & Qian, Yi & Qing Yang Hu, Rose. "*Security for 5G Mobile Wireless Networks*", IEEE Access, 2017.

[17] Michael Haus, Muhammad Waqas, Aaron Yi Dingy, Member, IEEE, Yong Li,"*Security and Privacy in Device-to-Device (D2D) Communication: A Review*", IEEE Communications Surveys & Tutorials, December, 2016.

[18] Yajun Chen, Xinsheng Ji, Kaizhi Huang, Jing Yang, Xin Hu, Yunjia Xu1,"*Artificial noise-assisted physical layer security in D2D-enabled cellular networks*", EURASIP Journal on Wireless Communications and Networking,2017.

[19] Bushra Ismaiel_, Mehran Abolhasany, David Smithz Wei Nix Daniel Franklin, "*Scalable MAC Protocol For D2D Communication For Future 5G Networks*", 14th IEEE Annual Consumer Communications & Networking Conference (CCNC),2017.

[20] Francesco Malandrino, Claudio Casetti, and Carla-Fabiana Chiasserini "*Toward D2D-Enhanced Heterogeneous Networks*", IEEE Communications Magazine, November 2014.

[21] Emad Abd-Elrahman, Hatem Ibn-khedher and Hossam Afifi, "*D2D Group Communications Security*", International Conference on Protocol Engineering (ICPE) and International Conference on New Technologies of Distributed Systems (NTDS),2015.

[22] Arash Asadi, Qing Wang, Vincenzo Mancuso, "*A Survey on Device-to-Device Communication in Cellular Networks*", IEEE Communications Surveys & Tutorials (Volume: 16, Issue: 4, Fourth quarter, 2014.

[23] Juho Lee, Younsun Kim, Yongjun Kwak, Jianzhong Zhang, Aris Papasakellariou, Thomas Novlan,Chengjun Sun, Yingyang Li,"*LTE-Advanced in 3GPP Rel -13/14:An Evolution Toward 5G*", IEEE Communications Magazine — Communications Standards Supplement ,March 2016.

[24] 3GPP (2015). 3GPP TS 36.306 (2015-03).

[25] Federico Boccardi, Robert W. Heath, Angel Lozano, Thomas L. Marzetta, Petar Popovski,"*Five disruptive technology directions for 5G*", IEEE Communications Magazine,Vol. 52,Issue 2,February,2014.

[26] Nan Yang, Lifeng Wang, Giovanni Geraci, G.,Jinhong Yuang," *Safeguarding 5G wireless communication networks using physical layer security*". IEEECommunications Magazine, April, 2015.

[27] Akhil Gupta, Rakesh Kumar Jha,"*A Survey of 5G Network: Architecture and Emerging Technologies*", IEEE Access, Vol. 3, 2015.

ISBN: 978-988-14047-9-4
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)