DOI: http://dx.doi.org/10.26483/ijarcs.v8i7.4265

ISSN No. 0976-5697

Volume 8, No. 7, July – August 2017

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

GRAY HOLE ATTACK ON HYBRID 5G NETWORK

Anshu Bhan
Centre of Computer Science and Technology,
Central University of Punjab, Bathinda,India

Surinder Singh Khurana
Centre of Computer Science and Technology,
Central University of Punjab, Bathinda,India

Abstract: 5G device to device communication is such a product of progressive thinking, a network that uses both LTE communication scenario in conjugation with Wi-Fi low band communication. The main idea for conjunction of two different types of network is based on the fact that base stations suffer large amount of traffic and tend to drop data and information in such cases. Apart from these facts another main stream goal is to provide security for such a communication technology. The network is based on the transitioning nodes, a set of cluster head communicates with another cluster head using base stations and nodes in between transfer from one cluster head to another. Gray hole attack is a situation in which the attacker inserts a malicious node into cluster head and steals information. This paper is based on the performance of 5G networks and effects of gray hole attacks on 5G networks.

Keywords: D2D Communication, Wi-Fi, In-Band communication, Out-Band communication, Hybrid architecture, 5G, Clustering

I. INTRODUCTION

Wireless data traffic has increased day by day over the past few years. Today's the cellular network mobile users require a much higher data rate than before [1]. The existing techniques can no longer satisfy users' needs due to the emergence of numerous daily routine applications.

D2D communication, which can reduce the load on the cellular infrastructure and also increase the spectral efficiency and considered to be a promising technique for the next generation cellular networks. Unlike the traditional communications, traffic has to go through the Base Station (BS) even if the users are within the short range of each other. In the D2D technique, UEs transfer data directly to each other without crossing the BS or a core network[2].

II. WIRELESS

A wireless word defined as having no wires. In network technology, wireless is the term used to describe any computer network where there is no physical wire between sender and receiver. It is connected by radio waves or microwaves to maintain communication[3]. A wireless network uses Network interface card and routers.

"G" in wireless refers to Generation

A. First Generation (1G)

The first analog cellular system which was started in 1980 which was first introduced in the USA[2], [4]. 1G was purely designed for voice calls with no consideration of data services. It allows the voice call in only one country. The speed of 1G was up to 2.4 kbps. It was first wireless communication. Its operating frequency is 800 MHz, and the carrier frequency is 30 KHz.

B. Second Generation (2G)

It is considered to be the first digital cellular network which was launched in 1991 in Finland and its data speed was up to 64 kbps. 2G was based on GSM (Global System for Mobile Communication). It is the digital version of 1G. It allows both voices as well as data. Its bandwidth is 25 MHz, and operating frequency for GSM 900 MHz, 1800 MHz and for CDMA 800 MHz and its carrier frequency is 200 KHz. It enables services as the text message, picture message, and multimedia message. It provides better quality and capacity.

C. Third Generation (3G)

It was introduced in 2000 in Japan. Data transmission speed is up to 2 Mbps. It provides faster communication, high web speed, more security, video conferencing, TV streaming, 3D gaming. Smart phone feature increased its bandwidth and data transfer rate to accommodate web based application and audio video files. Its bandwidth is 25 MHz[5], and carrier frequency is 5 MHz

D. Fourth Generation (4G)

It was introduced in 2009 in South Korea. Its speed is 100 Mbps to 1Gbps[2], [5]. To describe 4G basic term MAGIC:-

- **M** – Mobile Multimedia
- **A** –Anytime Anywhere
- **G** – Global Mobility Support
- **I** – Integrated Wireless Solution
- **C** – Customized Personal Services

Also known as Mobile broadband everywhere. It provides more security, high speed, high capacity, low-cost Per-bit. Its bandwidth is 100 MHz, and operating frequency is 850 MHz and 1800 MHz, and carrier frequency is 15 MHz[6].

E. Fifth Generation (5G)

5G (Fifth Generation Mobile and Wireless Networks) is a complete wireless communication without limitation, which brings us in real world wireless – World Wide Wireless Web (WWWW). 5G indicates the next major phase of mobile telecommunications standards beyond the 4G standards. In 5G we use the hybrid technology i.e. cellular network and Wi-Fi. It will be launched in 2020[6].

III. GRAY HOLE ATTACK

Gray hole attack comes from the set of active attacks these type of attacks are associated with dropping of packets by entering into the network through malicious means. In this the attacker initiates a malicious node into the network and then acts as legitimate node, but in the process it starts failing and

dropping the packets[7]. The basic strategy is to agree to work correctly but not working. Initially, the node performs correctly and replays true router response RREP messages to nodes that initiate router request RREQ packets[7]. Dropping the packets, gray hole attack is launched. Constantly in the connection, when the other nodes send the packets to malicious node thus marking the routing misbehavior.

IV. METHODOLOGY

The methodology to establish a hybrid 5G network consists of two types of technologies are:

- LTE Network Communication
- Wi-Fi Network Communication.

Various stationed nodes will be connected to the cluster head. Each cluster head has provision of two type of communication. Such that if the stationed node has to communicate to the other node of same network then Wi-Fi network will be used but if the stationed node has to communicate to the other network node then cluster head using the LTE network sends the data to the base station and then base station to the cluster head of corresponding network and then to the station node of the network[8], [9]. Once network selection will be taken place at the cluster head level then send the data through cluster head. But if cluster head behaves as a gray hole then it might drop the messages. For safe guarding of this we detect the malicious cluster head and alternate cluster head is selected. Till cluster head starts behaving in legitimate cluster head.

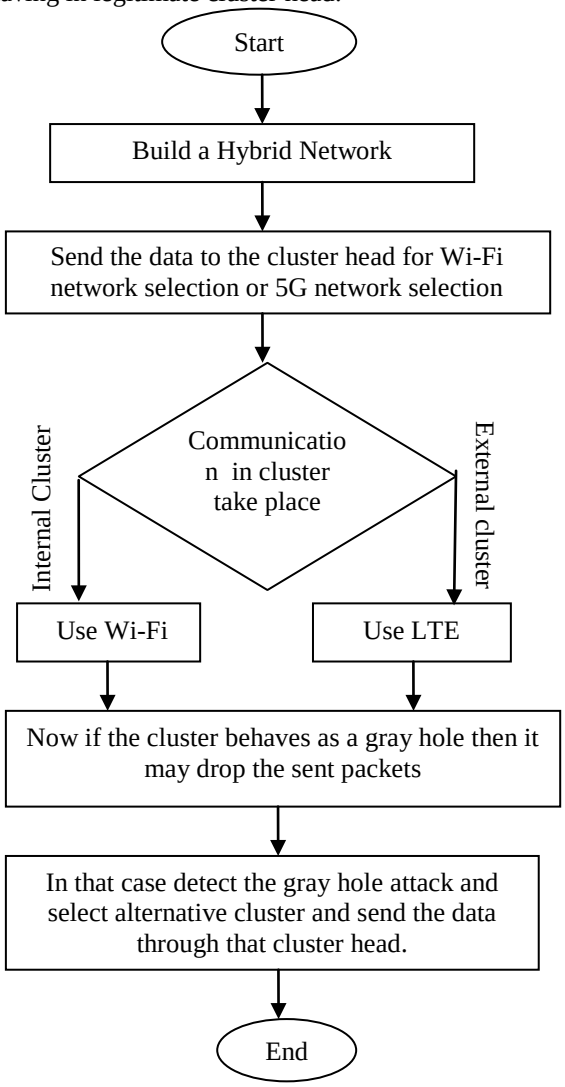

Figure 1 Flow chart of Hybrid network[10]

F. Generation of Gray Hole Attack in 5G Network

Gray Hole Attack in 5G Networks is simulated in Network Simulator NS3. In this simulation, gray hole attack is introduced in normal working of 5G Networks. As in gray hole attack, malicious node drops packets (more than 10% packet loss is considered as gray hole attack) randomly[11]. Therefore, concept of Random number generation is used in NS3 to simulate the scenario of packet drop in NS3. For gray hole attack simulation, cluster head which is depicted by class ap-wifi-mac drop packets randomly[12].

G. Detection of Gray Hole Attack

Once Gray Hole attack occurs in hybrid 5G networks, then, it is to be detected. Detection of gray hole attack is done by simulating technique of trust and packet loss[13]. In this technique, when data is transmitted on the path to the destination nodes from the source node, total packets which is received at particular node is counted, if there is any packet loss (more than 10% packet loss is considered as gray hole attack) the loss is informed to the source node, after this Source Node will transmit the packets again taking the another path for transmission[2], here with the total count of the packet it is also counted that, if the specified type of packets are dropped by nasty node, if this happens this is due to Active gray hole Attack.

H. Removal of Gray Hole Attack

If packet Loss is detected as per trust and packet loss technique, then it is solved by following another path through legitimate cluster head in hybrid 5G networks[8]. When source node is informed about packet loss and it is higher, then gray hole attack is detected. Another cluster head is used by specifying it in ap-wifi-mac class. Malicious cluster head is not used for transferring messages and new cluster head is used for packet delivery[6], [8], [14]. This technique successfully removes Gray hole attack in 5G networks

V. RESULTS

This paper present the effect of gray hole on 5G d2d communication. The same has been studied using an open source simulation libraries, Network Simulator-3 (ns-3). The main performance parameters considered are the throughput, packet delay and packet loss ratio. The performance is evaluated using two applications: BulkSend and UdpEchoClient.

I. Parameters using BulkSend Application

Different parameters have been analyzed like Packet delivery ratio, Packet loss, Throughput using BulkSend Application in ns3.

1) Packet Delivery Ratio

Packet delivery ratio using BulkSend Application is said to be 100% but since many deformities or obstacles are faced during transmissions. There stands a chance of fluctuation in this value. Figure 2 shows that the packet delivery ratio was 108 packets but after the network was under the gray hole attack the PDR dropped to 54 packets only.

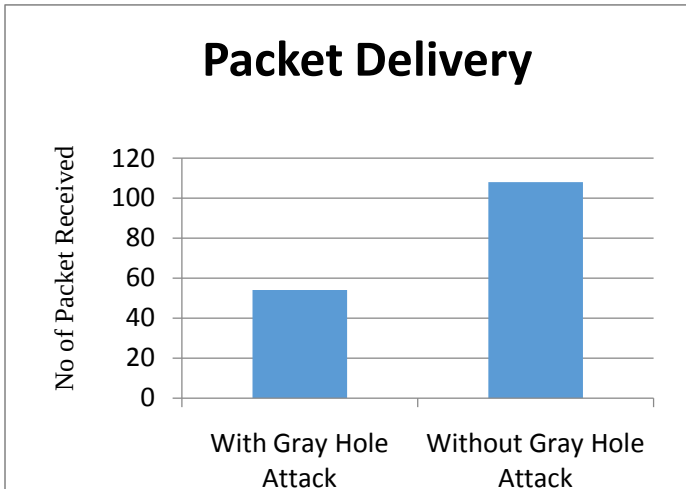

Figure 2 Packet Delivery using Bulksend Application

2) ***Packet Loss***

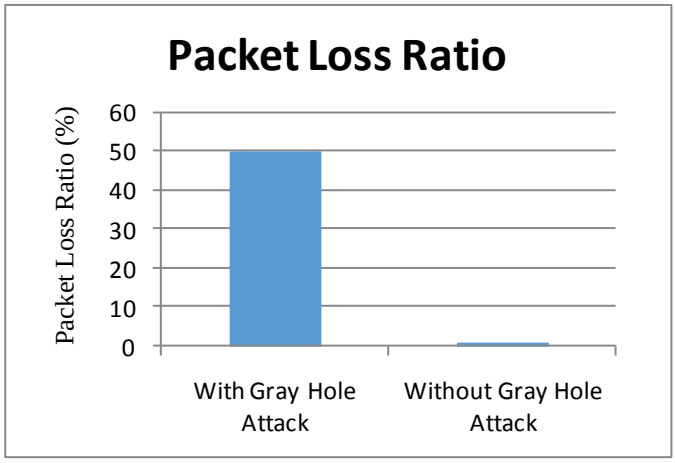

Figure 3 Packet Loss Ratio using Bulksend Application

Packet loss ratio using BulkSend Application is an important aspect as it describes the delivery performance for the network, more the loss more the harm to network performance. Figure 3 shows the packet loss ratio increasing as the network suffers the gray hole attack.

3) ***Throughput***

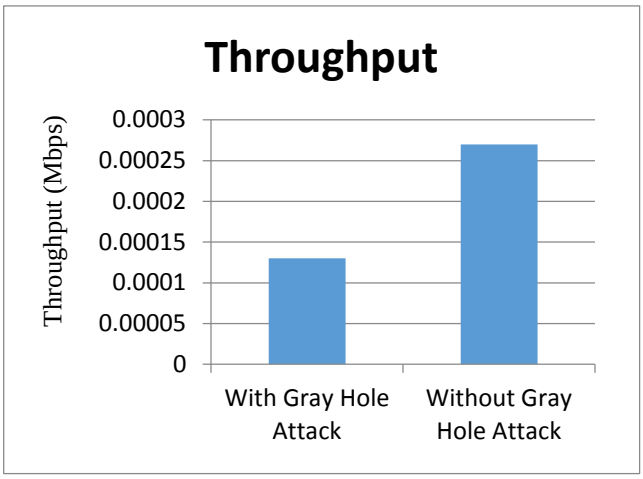

Figure 4 Throughput using Bulksend Application

Figure 4 shows that the throughput was higher when there was no gray hole attack on the network, but after the network was under the influence of gray hole attack the throughput decreased to 0.00013

J. Parameters using UdpEchoClient Application

Different parameters have been analyzed like Packet delivery ratio, Packet loss, Throughput with UdpEchoClient Application in ns3.

1) ***Packet Delivery Ratio***

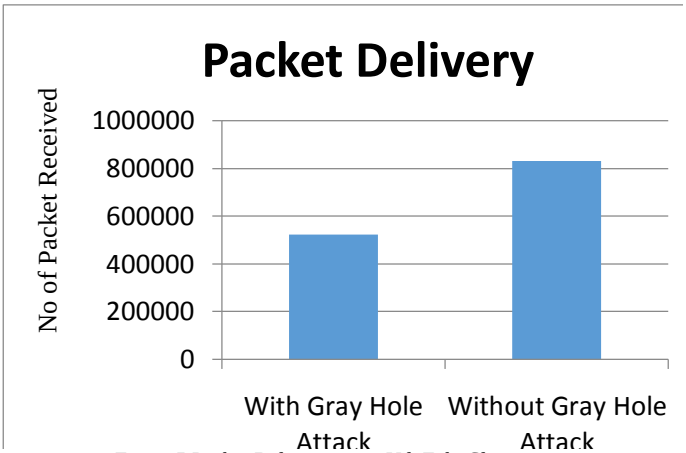

Figure 5 Packet Delivery using UdpEchoClient

Packet delivery ratio is said to be 100% but since many deformities or obstacles are faced during transmissions. There stands a chance of fluctuation in this value. Figure 5 shows that the packet delivery ratio was 830400 packets but after the network was under the gray hole attack the PDR dropped to 523152 packets only.

2) ***Packet Loss Ratio***

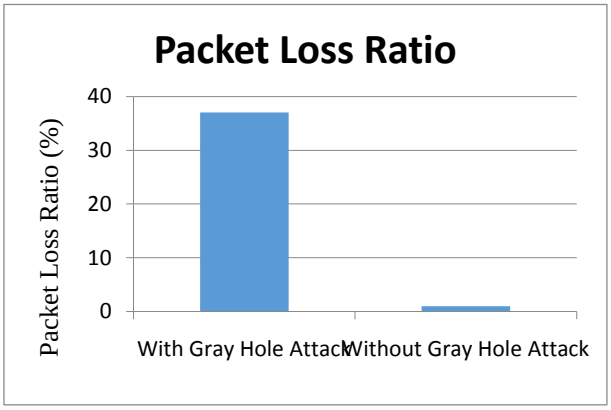

Figure 6 Packet Loss Ratio using UdpEchoClient

Packet loss ratio is an important aspect as it describes the delivery performance for the network, more the loss more the harm to network performance. Figure 6 shows the packet loss ratio increasing as the network suffers the gray hole attack.

3) ***Throughput***

Figure 7 shows that the throughput was higher when there was no gray hole attack on the network, but after the network was under the influence of gray hole attack the throughput decreased to 1.33

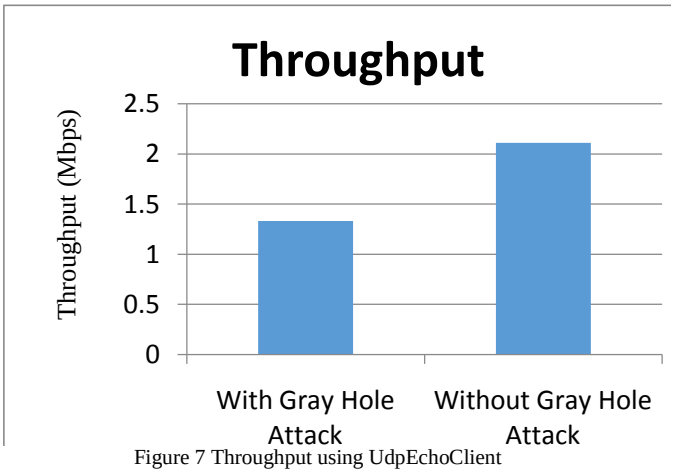

Figure 7 Throughput using UdpEchoClient

Figure 8 shows the scenario created in ns3 simulator for 5G network. Two cluster heads were constructed in the network scenario; out of which one of the cluster head possess two sub cluster heads. These cluster heads are then simulated to communicate.

```
'build' finished successfully (1m22.909s)
Flow 1 (10.1.1.1 -> 10.1.3.4)
  Tx Bytes:   830400
  Rx Bytes:   830400
  Throughput: 2.11182 Mbps
  Packet Loss Ratio: 0 %
Flow 2 (10.1.1.2 -> 10.1.3.4)
  Tx Bytes:   830400
  Rx Bytes:   830400
  Throughput: 2.11182 Mbps
  Packet Loss Ratio: 0 %
Flow 3 (10.1.1.3 -> 10.1.3.4)
  Tx Bytes:   830400
  Rx Bytes:   830400
  Throughput: 2.11182 Mbps
  Packet Loss Ratio: 0 %
vaio@vaio-VGN-CR12GH-B:~/ns3/ns-allinone-3.26/ns-3.26$
```

Figure 8 Communication without Gray Hole Attack using UdpEchoClient

This communication is presented as a simulated 5G network. In this network, the gray hole attack was implemented. This attack led to production of few effects over the previously created 5G network. Figure 9 shows the network statistics for the gray hole attack on 5G network.

```
Flow 1 (10.1.1.1 -> 10.1.3.4)
  Tx Bytes:   830400
  Rx Bytes:   523152
  Throughput: 1.33044 Mbps
  Packet Loss Ratio: 37 %

 Gray Hole Attack Detected


  Mitigating.....


  Alternate Cluster Head selected

Flow 1 (10.1.1.1 -> 10.1.3.4)
  Tx Bytes:   830400
  Rx Bytes:   830400
  Throughput: 2.11182 Mbps
  Packet Loss Ratio: 0 %
Flow 2 (10.1.1.2 -> 10.1.3.4)
  Tx Bytes:   830400
  Rx Bytes:   830400
  Throughput: 2.11182 Mbps
  Packet Loss Ratio: 0 %
Flow 3 (10.1.1.3 -> 10.1.3.4)
  Tx Bytes:   830400
  Rx Bytes:   830400
  Throughput: 2.11182 Mbps
  Packet Loss Ratio: 0 %
vaio@vaio-VGN-CR12GH-B:~/ns3/ns-allinone-3.26/ns-3.26$
```

Figure 9 Communication with Gray Hole Attack using UdpEchoClient

Figure 10 shows the scenario created in ns3 simulator for 5G network. Two cluster heads were constructed in the network scenario; out of which one of the cluster head possess two sub cluster heads using BulkSend Application. These cluster heads are then simulated to communicate.

```
Build commands will be stored in build/compile_commands.json
'build' finished successfully (10.603s)
Flow 1 (10.1.1.1 -> 10.1.3.4)
  Tx Bytes:   108
  Rx Bytes:   108
  Throughput: 0.000274658 Mbps
  Packet Loss Ratio: 0 %
Flow 2 (10.1.1.2 -> 10.1.3.4)
  Tx Bytes:   108
  Rx Bytes:   108
  Throughput: 0.000274658 Mbps
  Packet Loss Ratio: 0 %
Flow 3 (10.1.1.3 -> 10.1.3.4)
  Tx Bytes:   108
  Rx Bytes:   108
  Throughput: 0.000274658 Mbps
  Packet Loss Ratio: 0 %
```

Figure 10 Communication without Gray Hole Attack using BulkSend

This communication is presented as a simulated 5G network. In this network, the gray hole attack was implemented. This attack led to production of few effects over the previously created 5G network. Figure 11 shows the network statistics for the gray hole attack on 5G network

```
Build commands will be stored in build/compile_commands.json
'build' finished successfully (2.118s)
Flow 1 (10.1.1.1 -> 10.1.3.4)
  Tx Bytes:   108
  Rx Bytes:   52
  Throughput: 0.000132243 Mbps
  Packet Loss Ratio: 50 %

 Gray Hole Attack Detected


  Mitigating.....


  Alternate Cluster Head selected

Flow 1 (10.1.1.1 -> 10.1.3.4)
  Tx Bytes:   108
  Rx Bytes:   108
  Throughput: 0.000274658 Mbps
  Packet Loss Ratio: 0 %
Flow 2 (10.1.1.2 -> 10.1.3.4)
  Tx Bytes:   108
  Rx Bytes:   108
  Throughput: 0.000274658 Mbps
  Packet Loss Ratio: 0 %
Flow 3 (10.1.1.3 -> 10.1.3.4)
  Tx Bytes:   108
  Rx Bytes:   108
  Throughput: 0.000274658 Mbps
  Packet Loss Ratio: 0 %
```

Figure 11 Communication with Gray Hole Attack using BulkSend

VI. CONCLUSION

In this paper the main goal was to implement the 5G network simulation on network simulator (ns3) and check the effects of gray hole attacks on this network[15], [16]. The 5G network is implemented using two different kinds of frequency bands (licensed and unlicensed) which are further known as LTE (Long Term Evaluation) in combination with Wi-Fi networks. In 5G d2d communication, there is a possibility of an insecure exchange of information taking place. Gray hole attack takes advantage of this and captures the cluster head and turns it into a malicious cluster head, hence stealing information, dropping packets, etc. Under the influence of gray hole attack, 5G network losses its ability to work properly. During the simulation it was observed that the throughput and packet delivery ratio were adversely affected by gray hole attack. The emphasis is given on detecting the gray hole attack and then diverting the traffic from the malicious cluster head to the non-malicious cluster head in order to continue the proper working of the network.

VII.REFERENCES

[1] R. R. Brooks, "Wireless Sensor Networks: Architecture and Protocols," *Int. J. Distrib. Sens. Networks*, vol. 4, no. 3, pp. 286–286, 2008.

[2] A. Asadi, Q. Wang, and V. Mancuso, "A survey on device-to-device communication in cellular networks," *IEEE Commun. Surv. Tutorials*, vol. 16, no. 4, pp. 1801–1819, 2014.

[3] A. B. Karuppiah, J. Dalfiah, K. Yuvashri, S. Rajaram, and A.-S. K. Pathan, "A Novel Energy-Efficient Sybil Node Detection Algorithm for Intrusion Detection System in Wireless Sensor Networks," in *2014 3rd International Conference on Eco-friendly Computing and Communication Systems*, 2014, pp. 95–98.

[4] N. Yang, L. Wang, G. Geraci, M. Elkashlan, J. Yuan, and M. Di Renzo, "Safeguarding 5G wireless communication networks using physical layer security," *IEEE Commun. Mag.*, vol. 53, no. 4, pp. 20–27, Apr. 2015.

[5] P. Sharma, "Evolution of Mobile Wireless Communication Networks-1G to 5G as well as Future Prospective of Next Generation Communication Network," *Int. J. Comput. Sci. Mob. Comput. - not index*, vol. 2, no. August, pp. 47–53, 2013.

[6] P. Gandotra and R. K. Jha, "Device-to-Device Communication in Cellular Networks: A Survey," *J. Netw. Comput. Appl.*, vol. 71, pp. 99–117, 2016.

[7] Z. Lin, Z. Gao, L. Huang, C. Y. Chen, and H. C. Chao, "Hybrid Architecture Performance Analysis for Device-to-Device Communication in 5G Cellular Network," *Mob. Networks Appl.*, vol. 20, no. 6, pp. 713–724, 2015.

[8] N. Bhushan, Junyi 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 Commun. Mag.*, vol. 52, no. 2, pp. 82–89, Feb. 2014.

[9] P. Agyapong, M. Iwamura, D. Staehle, W. Kiess, and A. Benjebbour, "Design considerations for a 5G network architecture," *IEEE Commun. Mag.*, vol. 52, no. 11, pp. 65–75, Nov. 2014.

[10] M. Hicham, N. Abghour, and M. Ouzzif, "Device-To-Device (D2D) Communication Under LTE-Advanced Networks," *Int. J. Wirel. Mob. Networks*, vol. 8, no. 1, pp. 11–22, 2016.

[11] Q. C. Li, H. Niu, A. T. Papathanassiou, and G. Wu, "5G Network Capacity: Key Elements and Technologies," *IEEE Veh. Technol. Mag.*, vol. 9, no. 1, pp. 71–78, Mar. 2014.

[12] S. Dilek, H. Cakır, and M. Aydın, "Applications of Artificial Intelligence Techniques to Combating Cyber Crimes: A Review," *Int. J. Artif. Intell. Appl.*, vol. 6, no. 1, pp. 21–39, 2015.

[13] K. Giotis, G. Androulidakis, and V. Maglaris, "A scalable anomaly detection and mitigation architecture for legacy networks via an OpenFlow middlebox," *Secur. Commun. Networks*, vol. 9, no. 13, pp. 1958–1970, 2016.

[14] C.-X. Wang, F. Haider, X. Gao, X.-H. You, Y. Yang, D. Yuan, H. Aggoune, H. Haas, S. Fletcher, and E. Hepsaydir, "Cellular architecture and key technologies for 5G wireless communication networks," *IEEE Commun. Mag.*, vol. 52, no. 2, pp. 122–130, Feb. 2014.

[15] A. Gupta and R. K. Jha, "A Survey of 5G Network: Architecture and Emerging Technologies," *IEEE Access*, vol. 3, pp. 1206–1232, 2015.

[16] A. Adnan, M. M. Phil, C. Science, and G. Lahore, "Comparative Studies of 3G , 4G & 5G Mobile Network & Data Offloading Method a Survey," *IJRIT Int. J. Res. Inf. Technol.*, vol. 3, no. JUNE, pp. 421–427, 2015.