MALICIOUS NODE IDENTIFICATION FOR D2D COMMUNICATION IN 5G CELLULAR NETWORKS

Pratibha[1], Prof. (Dr.) A.K. Goel[2], Er. Nikita Sehgal[3]
[123]Department of Electronics and Communication, GZSCCET, MRSPTU, Bathinda, India

Abstract: 5G network system is the option for better coverage, capacity and spectral efficiency. Overall targets for the 5G network are to have higher throughput per area per user with lower latency. 5G can be the answer to ever growing number of users to their growing demands. The main focus is on implementation of D2D communication which reduces burden on cellular infrastructure and increases the spectral efficiency. Unlike the traditional one, traffic has to go to the base station first even if the users are within short range of each other. Another important factor is security. A network suffers from various types of attacks especially a network like 5G which works in unlicensed spectrum A technique is being proposed for detection of malicious node, a kind of trap method is used for the detection of malicious nodes. When the grey node is detected due to the trap, an alarm is triggered to make the other nodes aware of malicious nodes. So, the network performance has been checked under three condition i.e. when the network is in ideal state (WITHOUT GREY NODE), affected from the attack (WITH GREY NODE) and network after attack (REMOVED GREY NODE). The considered parameters are Throughput, Packet delivery Ratio, Delay, and Success rate. These parameters have shown the considerable improvements as compared to the network suffering from the grey hole attack.

Keywords: Grey Hole, 5G, Hybrid.

I. INTORDUCTION

In the fifth generation cellular network the integrated technologies is leading in both architectural and component design changes. The base station centric architecture of cellular system has changed intelligence at the device side by exploiting the different layers of protocol by using D2D. Device to Device (D2D) communication is the new feature of 5G to reduce the increasing traffic and offload the data from the user equipment (UE). This communication is categorized into In-band and Out-band based on the spectrum in which the communication occurs. In-band communication has the high control over licensed spectrum in which either they share the same network or have dedicated spectrum. On the other hand in Out-band communication, it eliminates the interface between D2D and cellular link. WiFi or Bluetooth is being used for the Out-band. Both of these technologies allows an electronic device to exchange data on low power, low cost for shorter range and enables D2D connections in unlicensed bands [1]. Another important factor is security. A network always suffers from various types of attacks, 5G which is working in unlicensed spectrum. During the grey hole attack, the malicious or unwanted nodes distract the data packets. They show them fake shortest and the freshest route for the destination node so that sender will forward all its data packets to the destination. When grey node receives the data packets, it will drop packets to create a Denial of service attack and processes to extract information. The specialty of this kind of attack is it drops the packets for particular time interval and after that it behaves like normal node so, it's difficult to detect grey hole. A technique is being proposed for detection of malicious node, a kind of trap method is used for the detection of malicious nodes. When the grey node is detected due to the trap, an alarm is triggered to make the other nodes aware of malicious nodes.

II. RELATED WORK

The status of 3rd Generation Partnership Project (3GPP) standardization is discussed in [1]. It defined a set of application scenarios for the D2D communications in 5G network. It used models of 3GPP i.e. long term evolution (LTE) and WiFi that interfaces in analyzing the power consumption from infrastructure and user device provisions which indicated that with latest radio interface, the best option for the energy saving was the minimization of active interface and sending the data to the best possible data rate.

In [3] discussed about the Fifth generation (5G) cellular networks could include millimeter wave (mmWave) for communication by which it gains the advantage of extensive frequency reuse and directive propagation. The integration of mmWave and Device to Device technology could improve the performance, spectral efficiency. The complexity was decreased as the resources to overlay mode. Two problems were addressed in this paper. First, assign the resources to the overlay mode which was solved by using quadratic program. While the next problem was formulated to maximize system capacity for overlay mode i.e. solved using heuristic algorithm.

In [4] implementation of Scalable admission and power control methods for the Device to device communications which underlay's the cellular networks to increase the reuse

of frequency and network capacity while maintaining its QoS for all users has been done. The aim of the proposed methods was to maximize the number of links under QoS for maximizing reuse of network frequency for practical 5G multi cell environment.

How to handle the interference explosion and optimized the radio resources allocation discussed in [5]. It proposed that enhance the interference coordination for the ultra-dense small cells which managing the hotspots of traffic and high mobility. It also satisfied the operator‘s requirement for profitable network infrastructure.

In [19] discussion about the Performance parameters of 5G wireless cellular communication systems is done. It represented the capacity, data rate, spectral efficiency, latency, energy efficiency, and Quality of service. A 5G wireless network architecture showed with massive MIMO technology, network function virtualization (NFV) cloud and D2D communication. Some communication technologies, like wifi, Small cell, Visible light communication and millimeter wave communication technologies have explained in terms of better quality and increased data rate for inside users and at the same time it reduces the pressure for the outside base stations. Some technologies have been discussed that could be used in 5G wireless systems to fulfils the demand like massive MIMO in D2D communication and interference management, its spectrum sharing with the cognitive radio, ultra dense networks, multi radio access technology, full duplex radios, millimeter wave communication and Cloud Technologies in general with radio access networks.

Mode selection techniques and clarifying its importance is discussed in [2]. Mode selection is the technique to choose whether two devices would communicate through D2D via using dedicated or shared resources rather than via the BS. It proved that D2D has higher SINR than cellular mode. In addition it presented mode selection and showed that this technology raise network performance by mixing cellular and D2D mode together.

In [11] discussion of Two typical networks that covered use cases of D2D communication has done . It proposed three novel key exchange protocols which involve only the two User equipment and the eNode B(enabled node). These proposed protocols addressed the typical vulnerability of D2D i.e., the man in the middle (MITM) attack. These proposed protocols were in increasing order of security and also examined the performance of the proposed protocols in comparison with existed protocols through numerical results. By numerical results it is clear that the proposed protocols have low computational time and low communication overhead in comparison to existed key exchange protocols for D2D communication. These proposed protocols are practically implementable for D2D communications in 5G cellular networks.

In [12] implementation of How disaster management could benefit from recent advances in the wireless communication technologies and protocols, especially mobile technologies and devices is done. The paper discussed about various potential emerging wireless communication technologies about 5G, D2D, 4G/LTE, and software defined radio for disaster situations. It focused on the use of ubiquitous mobile devices and applications in disaster situations.

An enhancement of scheme in order to avoid initial interaction discussed in [20]. In this stereotypes to be used in a place which were created by each user, but rather than exchanging profile information each one of such stereotypes were used to create an encryption key. These keys were created using attribute-based encryption on the basis of attributes of the stereotypes and the values defined by user. This key was later used to communicate between co-located devices. The usage of this encryption scheme allowed users to communicate with other trusted users without distributing the encryption key. Following this scheme it first classifies the place where users were currently located.

III. D2D ARCHITECTURE

In this network integration of several technologies can be done like LTE and WiFI. Device-to-device (D2D) communication which can enable the devices to communicate directly with other devices without any communication infrastructures like base stations. Bluetooth and WiFi-Direct are the two D2D techniques that can work in the unlicensed spectrum. In this hybrid network, D2D architecture and its cluster formation with the help of Bluetooth interface and WiFi interface. This scenario includes one BS and two Clusters. Inside that cluster all the UEs transfer traffic to each other directly via the WiFi-Direct interface. Each cluster has its own cluster head which carries out the D2D communications in the In-Band mode[1].

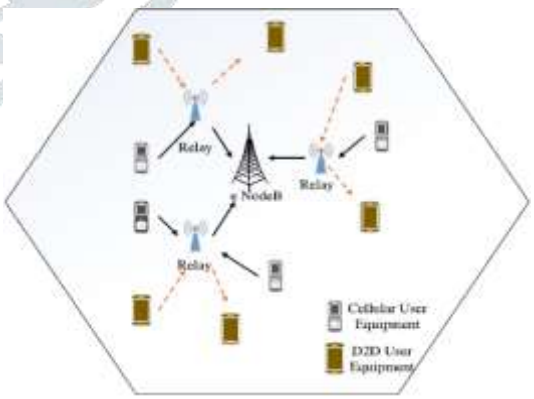

Fig. 1 D2D communication[3]

IV. OUTBAND CLUSTER FORMATION VIA BLUETOOTH AND WIFI

A. Bluetoth-Now a days, mobile devices are running with limited battery power. This makes it essential to have such scheme which can be used for reducing power consumption. In the formation of out band cluster it used blue tooth based communication. Bluetooth based communication would take less power as compared to the cellular communication

so, lower power of the Bluetooth interface is used as primary source for cluster formation. Each cluster consists of its own cluster head and various nodes which are mobile User Equipments (UEs). These user devices communicate with various types of interfaces like WiFi-Direct interface, Bluetooth and cellular network. In this an assumption has been made that each UE is able to measure its residual charge and signal to interference plus noise ratio(SINR). Each cluster has one Cluster Head i.e. enable to calculate all the Cluster Normal Members' (CNM) Intent Value and CNMs they are time synchronized with the CH. A mobile UE initiates a D2D communication and it will detect the message broadcasted periodically by cluster. If the UE detects message within maximum time interval *T*, it shows that cluster exist nearby. Otherwise, there is no cluster in that available range. Then the UE initiate to form cluster itself. [13].

When the cluster is around and new user want to make a D2D communication then it will open its Bluetooth interface first and it will start its detection and analyzing for the CH's broadcast messages. The other mobile UE will send the requested message to the CH to join the cluster. When the cluster head will receive the request it will response to the User Equipment. If the mobile UE has permission to join the cluster then it will send confirmed message to the cluster head, now the Cluster Head will add new joining UE's information into list. Else, if the mobile UE received the declined response, it will send the request again after the time interval T. If there is no cluster around, the UE will not be able to detect the broadcast message in the time interval T, then UE will set himself as the CH and send broadcast message.

B. WiFI- According to cluster structure, WiFi Direct transmissions between CH and CNMs are carried with synchronized time by the WiFi Direct interface. When the CNM required D2D communication, it will open up the WiFi Direct interfaces and send data packets in the given slot. When CH received and analyzed the packet headers and data packets, they will be retransferred back into the cluster by CH with the help of WiFi Direct interface if receiver is in the same cluster with transmitter. Else, the data packets will retransfer to other CH on the same cellular spectrum

V. INBAND CLUSTER FORMATION

In Band D2D mode is important part in Hybrid Band D2D communication ,there are two clusters cluster 1 and cluster 2, provided that CH 2 has downloaded several videos from the BS already. There is a chance i.e. one or more CNMs from cluster 1 want to share the same videos and then BS allocates resources for CH1 and CH2 to start D2D communication. In the mean time CH1 will broadcast the videos for its CNMs. This procedure will decrease the load and also increase the system throughput and also minimize the transmission delay. Before the D2D transmission, the link setup formation of D2D communication needed to be completed. When the D2D link setup is completed, the mobile UE will begin to transfer data packets by the link. In Band D2D communication is able to reuse the uplink or downlink resources for transferring data packets. Most of the work about In Band D2D communication focuses on the resource allocation system and interferences from D2D users to the cellular network. Else, this work focuses on the improvement in system performances in the hybrid network of D2D communications.

VI. VULNERABILITIES IN 5G

This security issues are considered in 5-G because of its characteristics like as vulnerability of channels, nodes, and dynamically changing topology, absence of infrastructure. In 5-G, a mobile node always have some limitations with respect to its bandwidth, computing power, and battery which lead to application-specific tradeoffs among security and resource consumption of mobile device[7].

A. Grey hole attack-Grey hole attack is the type of denial of service attack. During attack, the router which is kind of mesh will not behave well and a subset of packets which are being forward and handle by receiver but leave by the network. Black hole and Grey hole attacks are the two attacks in wireless mesh network which can spoil the network topology and degrades the network performance In grey hole attack when the RREP (route request packet) message is generated by source node, but received by malicious node then it will generate a fake RREP and put a very large value on Destination Sequence Number field and uncast it for the source node. While receiving RREP, the source will start forwarding data packets to malicious nodes, by assuming that it has have shortest path to the destination and ignore all other RREP packets. The all data packets which are received by malicious node not get forwarded by it to any other nodes. This attack is called grey hole attack because all data packets are dropped by malicious node but they all are dropped for some specific time duration the source node.

B. Route Discovery –During route Discovery grey hole node always reply for RREQ sent by Sender it doesn't check his routing table as shown in the Fig no 2. This method is used to trap RREQ for trapping the malicious node and used promiscuous mode to monitor malicious behavior of node. In this sender sends the trap RREQ which contains destination address i.e. not exists in the network so when grey hole node receive RREQ it will not check his own routing table and send reply to the source node, after receiving Fake RREQ response, sender node records source of fake RREP and add it to its malicious list and inform it to all other nodes then all other nodes isolate the malicious node from their routing table. Now sender starts the actual path discovery and broadcasted RREQ to all his neighbors for routing to actual destination, if any malicious node is left in network then this node can be detected by monitoring phase. This phase actually detects signal.

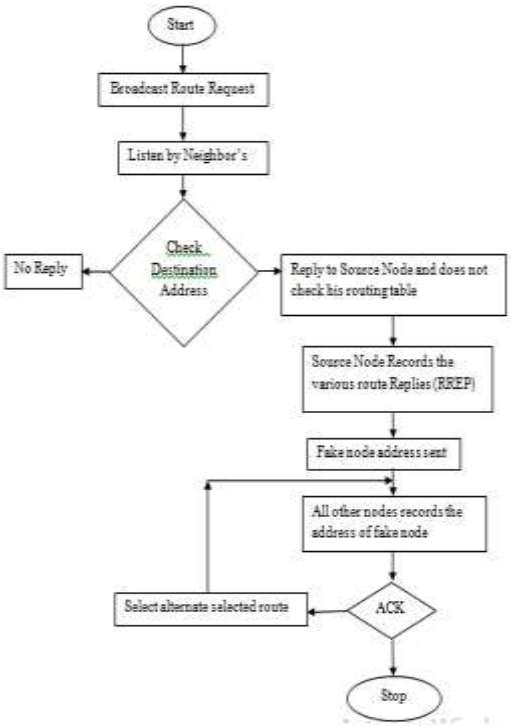

Fig.2 Flowchart of route recovery [6]

C. Monitoring phase- In this phase all the node will work in promiscuous mode means all the nodes are monitoring their neighboring node activities, if there is malicious node left in network, it would not forward data to next node, so packet forwarding ratio get decreased if this ratio is lesser than the threshold value monitoring node will immediately send alert message to the source node then source node discards its entry from routing table.

VII. RESULT ANALYSIS

A. Network Parameters- The applied network parameters in this dissertation are following where as AODV (Ad hoc On-Demand Distance Vector) and TCP(Transmission Control Protocol/Internet Protocol) etc.

Table 1 Network Configurations

Parameters	Value
Routing Protocol	AODV
Communication protocol	TCP
Delay	1 Sec
No. of nodes per cluster	10
No. of base station	1
Data transfer rate under wifi	2Mbps
Data transfer rate under 5G cellular	1 Gbps

B. Performance Parameters- Parameters are calculated under the influence of 10, 30 and 50 nodes.

Throughput -It is number of packets delivered to the destination per unit interval of time.

Throughput=Total Packet Received /Total Time[14]

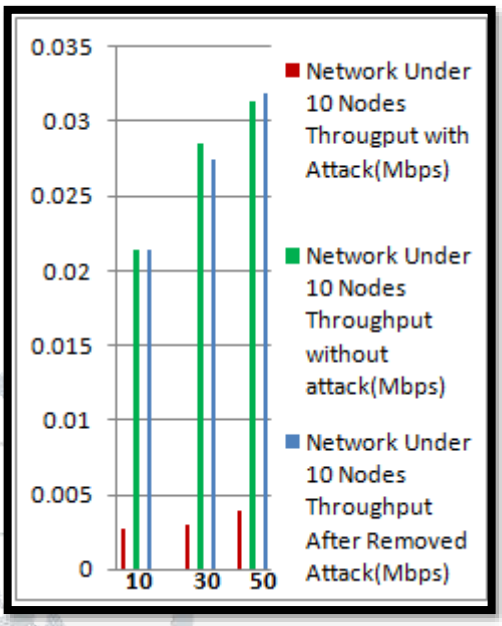

Fig. 3 Throughput comparison

Fig. 3 shows the throughput comparison at the 10, 30 and 50 nodes. This graph shows the considerable improvement in the throughput after and before the attack. Overall improvement in the throughput is 13%.

Delay-It is total delay produced to deliver the packet from source to destination.

Delay=End Time -Start Time

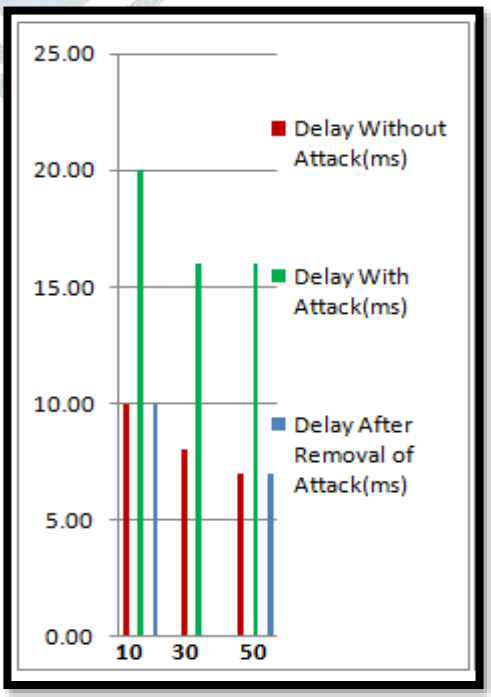

Fig. 4 delay comparison

Fig. 4 shows the delay comparison at the 10, 30 and 50 nodes. This graph shows the considerable improvement in the delay after and before the attack. Overall improvement in the delay is 18%.

Packet Delivery Ratio -It is total number of packets delivered to packet sent against the received destination.
Packet Delivery Ratio=Packet Sent/ Packet Received[15]

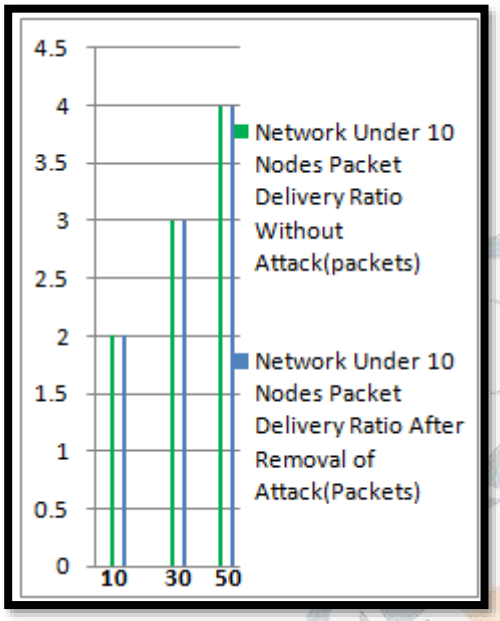

Fig. 5 packet delivery ratio comparison

Fig. 5 shows the packet delivery ratio comparison at the 10, 30 and 50 nodes. This graph shows the considerable improvement in the packet delivery ratio after and before the attack. Overall improvement in the packet delivery ratio is 10%.

Success Rate (SR)-It is the fraction of the attempts to send that result in a connection to the success number
Fig. 5 shows the success rate comparison at the 10, 30 and 50 nodes. This graph shows the considerable improvement in the success rate after and before the attack. Overall improvement in the success rate is 16%.

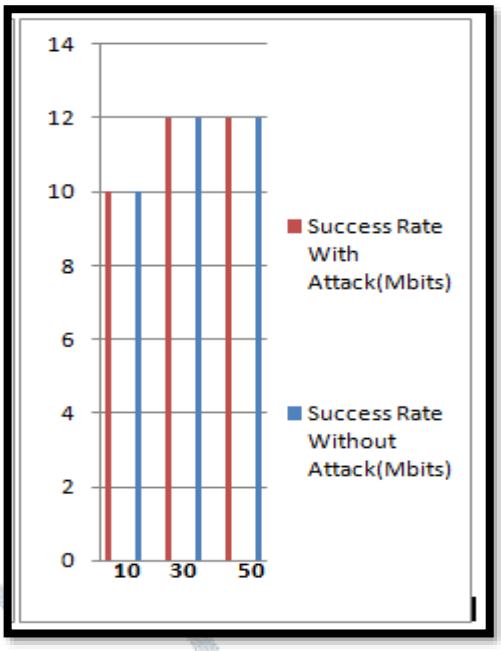

Fig. 6 success rate comparison

VIII. CONCLUSION

The main focus is on implementation of D2D communication which reduces burden on cellular infrastructure and increases the spectral efficiency. Traffic has to go to the base station first even if the users are within short range of each other. By D2D network UEs transfer data directly to each other without traversing the base station. This communication is categorized into In-band and Out-band based on the spectrum in which the communication occurs. Another considerable factor is security. A network suffers from various types of attacks especially in network like 5G which works in unlicensed spectrum so, the network performance has been checked under three condition i.e. when the network is in ideal state (WITHOUT GREY NODE), affected from the attack (WITH GREY NODE) and network after attack (REMOVED GREY NODE). The conclusion is based on the parameters Throughput, Packet delivery Ratio, Delay, and Success rate by varying the value of number of nodes. These parameters have shown the enhanced improvements as compared to the network suffering from the grey hole attack.

IX. FUTURE WORK

In the future work, more intelligent cluster head algorithm which considers more factors should be developed. It would be rather interesting to focus on the D2D relay based on the cluster and the application of this hybrid- architecture D2D concept could be extended and analyzed. Second aspect is detection of gray hole attack in D2D hybrid network. This type of network is highly prone to various kinds of attacks. In future various other active and passive attacks can attack the network.

REFERENCES

[1] Marko Hoyhtya, Olli Apilo and Mika Lasanen, “Review of Latest Advances in 3GPP Standardization: D2D

Communication in 5G Systems and Its Energy Consumption Models", Future Internet, vol.10, issue 3, 2018.

[2] Hanan H. Hussein and Yong Li, "A Survey Of Millimeter Wave (Mmwave) Communications For 5G: Opportunities And Challenges", IEEE, vol. 12, issue 4, pp 345-355,2017.

[3] Gadiraju Divija Swetha and Garimella Rama Murthy, "Selective Overlay Mode Operation for D2D Communication in Dense 5G Cellular Networks", IEEE Symposium on Computers and Communications, pp.1-7, 2017.

[4] Daniel Verenzuela and Guowang Miao, "Scalable D2D Communications for Frequency Reuse 1 in 5G", IEEE Transactions on Wireless Communication, vol.16, 2017.

[5] Soumaya Hamouda, "Advanced Radio Access Solutions for the New 5G Requirements", 5G in Future Africa, 2017.

[6] Othmane Nait Hamoud, Tayeb Kenaza and Yacine Challal, "Security in Device-to-Device communications (D2D): a survey", HAL, 2017.

[7] Amit Rathee, Manu Phogat, Mukesh, "Future Trends in 5g Wireless Communication: A Survey", IEEE Access, vol.7, issue 7, pp 57-64, 2017.

[8] Georgios Katsinis, Eirini Eleni Tsiropoulou and Symeon Papavassiliou, "Multicell Interference Management in Device to Device Underlay Cellular Networks", Future Internet, vol.9, issue 3, pp890-900,2017

[9] V. K. Tonk, V. K. Dwivedi2 and P. K. Yadav, "Coded-Cooperation based Multi-Relay Algorithm for Device-to-Device Communication in 5G Cellular Networks", Indian Journal of Science and Technology,vol.10,issue4,2017

[10] S K Biswash and D N K Jayakody, "The Device Centric Communication System for 5G Networks", International Conference on Information Technologies in Business and Industry, vol.3,pp1-7,2016.

[11] Michael Haus, Muhammad Waqas and Aaron Yi Ding "Security and Privacy in Device-to-Device (D2D) Communication: A Review", IEEE Communications Survey, vol.5, issue 6, pp 123-130,2016.

[12] Ravindranath Sedidi ,"Device-To-Device Communication In Cellular Networks: A Survey", ElseVier , vol. 2, issue 7, pp 567-577,2016.

[13] Krishna Kumar Bhargava and Suresh Gawande, "Analysis of D2D communication in 5G network", International Research Journal of Engineering and Technology, Vol. 3, issue 6, pp 626-630,2016.

[14] Ruksar Fatima, Rohina Khanam and Shaik Humera Tauseef, "Designing a framework for Device-to-Device Communications In LTE-Advanced Network", International Journal on Emerging Technologies, vol.3 issue 7, pp 386-392, 2016.

[15] Mohammed Syed Dar, Pradeep Sharma and Priyanka Tiwari, "Efficient Scheduling For D2D Communication in 5g Networks", International Research Journal of Engineering and Technology, vol. 3, issue 5, pp 511-517, 2016.

[16] Magri Hicham, Noreddine Abghour And Mohammed Ouzzif, "Device to Device (D2D) Communication Under LTE-Advanced Networks", International Journal Of Wireless & Cellular phone Networks (IJWMN) , Springer, vol. 8, issue 9, pp 234-240, 2016.

[17] Miloud Bagaa, Adlen Ksentinix, Tarik Taleb, Riku Jantti, Ali Chelli and Ilangko Balasingham, "An efficient D2D-based strategies for Machine Type Communications in 5G cellular phone systems" ,Technology and Innovation, vol. 4, issue 3, pp 1-6, 2015.

[18] Pirkko Wahlström, "Device-to-device communications for 5G Radio Access Networks", Aalto University School of Electrical Engineering Department of Communications and Networking, 2015.

[19] Jian Qiao, Xuemin (Sherman) Shen, Jon W. Mark, Qinghua Shen, Yejun He, and Lei Lei, "Enabling Device-To-Device Communications In Millimeter-Wave 5G Cellular Networks", IEEE Communications Magazine,vol. 9,issue 3,pp 45-55,2015.

[20] Akhil Gupta and Han-Chieh Chao, "Hybrid Architecture Performance Analysis For Device to device Communication In 5G Cellular Network",IEEE, vol. 20, issue 6, pp 713–724,2015.

[21] Eitan Altman, Noreddine Abghour and Mohammed Ouzzif, ,"DEVICE-TO-DEVICE (D2D) Communication Under LTE-Advanced Networks", International Journal Of Wireless & Mobile Networks (IJWMN) ,Springer,vol. 8, issue 9, pp 234-240,2015.

Author' s profile

.Ms. Pratibha pursed Bachelor of technology from Punjab Technical University, in 2014. She is currently pursuing Master of technology in Electronics and communication in Giani Zail Singh Campus College of Engineering and Technology, Bathinda. Her main research work focuses on 5g security system[1]

Dr. Ashok Kumar Goel professor and head depatment of electronics and communication in Giani Zail Singh Campus College of Engineering and Technology, Bathinda. He has experience of 31 years in teaching. He has been the mentor of many M.tech and P.hD students and have multiple papers published in various reputed international journals and conferences. His main area of research/specializations is in soft computing, wireless communication, and big data[2].

Ms. Nikita Sehgal receivedher M.Tech in ECEfrom Punjabi University, Patiala and B.Tech from IKGPTU, Kapurthala. She is currently working as Assistant Professor in Department of ECE, Giani Zail Singh Campus College of Engineering and Technology, Bathinda. She has guided many M.Tech thesis and have multiple paper published in reputed international journal and conferences. Her main

research work focuses on wireless sensor networks. She has 4 years of teaching experience[3].