MALICIOUS NODE IDENTIFICATION IN HYBRID ARCHITECTURE PERFORMANCE ANALYSIS FOR DEVICE TO DEVICE COMMUNICATION IN 5G CELLULAR NETWORK

[1]Er. Sidharth,[2]Mr.Ashish Sharma
Department of Computer Engineering
Maharaja Agrasen Institute of Technology, Rohini
Delhi, India.siddharthmittal1995@gmail.com

Maharaja Agrasen Institute of Technology, Rohini
Delhi, India.ashish@mait.ac.in

Abstract: ***Cellular network uses wireless channel for transmission of both analog and digital data. As the technology in the cellular communication is growing the more data transmission requirements remains. For fulfilling the user needs for transmitting the multimedia data there requires 5G technology. This way high bandwidth transmission is taking place using 5G spectrum. While communication for efficient usage of the frequency spectrum there is a need of hybrid band. While selects dynamically that if the node to whom the communication is taking place belongs to same cluster then WiFi spectrum is used. But if the communication to the outside node of other cluster then the cellular spectrum will be used this way highly growing demands can be meet. But as the technology is growing there are various security threats. In current researched network there is chance of gray hole at the cluster head level. Such that few random data packets can be dropped. This will downgrade the network performance. In current project the identification of the malicious node is taking place. The network performance is measured on various parameters. So that network performance can be upgraded.***

Keywords:5G,Cellular,GrayHole,Active Attack.

I. INTRODUCTION

Visions for the 5G mobile and wireless communication systems forecast growing traffic volumes and increasing number of mobile devices. Traffic volumes in wireless communication have grown during the last years, and the growth is expected to continue also in the future. Traffic volumes beyond the year 2020 can be even 1000 times higher than traffic volumes of today. Future cellular networks will become denser with small cells. Compared to traditional macro cellular systems multi-layered networks with macro-cell layer covering relays, pico-cell and femto-cell layers, is becoming one option for better coverage, capacity and spectral efficiency. Overall targets for 5G systems are higher throughput per area and per user, and lower latency. The 5G systems will support huge amount of devices, and with energy consumption lower compared to current systems. D2D communication is seen as one answer to growing demands for future mobile and wireless communication systems. D2D might offer higher data rates and lower latency due to the short distance between the D2D pair. D2D communication is also energy efficient as no data communication via Base Station (BS), and thus also the traffic loads of BS decreases.

D2D communication will be network controlled or not network controlled when out-of-coverage, and D2D will (re)use the same licensed spectrum as the cellular links. D2D communication takes place directly between a D2D pair without base station controlling the communication. D2D communication can also be used in areas out-of-coverage or when cellular network fails, mainly for public safety purposes.

Currently Long Term Evaluation (LTE) is missing direct device-to-device communication function. 5G is challenged by broadband requirements such as video streaming and the Internet of Things that require low signaling overhead and quality of service (QoS) with higher traffic volume and bandwidths. However the mobile network control plane can be attacked by short and frequent communications that take advantage of vulnerabilities in signaling such as paging , service requests and radio resource control (RRC) . Such attacks can compromise a large number of mobile devices, or can target a list of mobiles by carefully timing the transmissions. Furthermore, signaling storms can be the result of malfunctioning apps that repeatedly establish and tear-down data connections with a serious effect on the QoS of the network control plane , and there have been frequent industry reports about this matter . Similar events have also been observed for mobile devices that seek to connect to Cloud services.

1.1 SECURITY ISSUES FOR 5-GS

This security issues are to be considered in 5-GS because of its characteristics like vulnerability of channels, nodes, absence of infrastructure and dynamically changing topology. In 5-Gs, a mobile node has some limitations with respect to bandwidth, computing power, and battery that can lead to application-specific tradeoffs between security and resource consumption of the mobile device. However, to do this intermediate node achieves no benefits. So there may be a possibility that some nodes refuse to forward packets and thereby decrease the efficiency of the network in term of throughput and packet delivery ratio. However, malicious behavior of the nodes is selfishness. A selfish node may try to save their resources like battery power and computation ability by not participation in network operation like data forwarding with

increasing the number of malicious nodes, there may be result of making a non-collaboration environment between other nodes and also affected the network performance they do not correctly process the network packets. Therefore, ensure that everything is correctly working in the network to support overall security and know how an insider malicious node is able to attack the wireless 5-Gs. Vulnerabilities of operating systems and upper layer applications that belong to user programs such as databases, browsers or client-server applications are not considered as a security issue for 5-Gs. In 5-Gs, there are different type of attacks that belongs to different network layers such as physical layer, medium access control layer, network layer and transport layer.

1.2 ATTACKS IN 5-G'S

Any attack on ad-hoc networks can be categorized as active and passive attacks. In an active attack, the misbehaving node actively disturbs the normal operation of the network with attempts to alter or destroy the data being exchanged in the network. It can also be classified into two categories, external attacks and internal attacks. External attacks are carried out by nodes that do not belong to the network. These attacks can be prevented by using standard security mechanisms such as encryption techniques and firewalls. Internal attacks are carried out by compromised nodes that are actually part of the network. Since the attackers are already part of the network as authorized nodes, internal attacks are more severe and difficult to detect when compared to external attacks. In passive attack the malicious entity only listens to the traffic without disturbing proper operation of the network. An attacker is also able to interpret the data gathered through snooping to violet confidentiality requirement. Detection of passive attacks is
Very difficult since the operation of the network it does not get affected. In 5-Gs, the common attack in 5-Gs is discussed below.

1.2.1 Passive Eavesdropping

An attacker can listen to any wireless network to know what is going on in the network. It first listens to control messages to infer the network topology to understand how nodes are located or are communicating with another. Therefore, it can gather intelligent information about the network before attacking. It may also listen to the information that is transmitted using encryption although it should be confidential belonging to upper layer applications. Eavesdropping is also a threat to location privacy. An unauthorized node can notice a wireless network that exists within a geographical area, just by detecting radio signals. To combat this, traffic engineering techniques have been developed.

1.2.2 Gray hole Attack (Routing Misbehavior)

Gray whole attack is an active type of attack, which lead to dropping of messages. Attacking node first agrees to forward packets and then fails to do so. Initially the node behaves correctly and replays true RREP messages to nodes that initiate RREQ message. This way, it takes over the sending packets. Afterwards, the node just drops the packets to launch Black Hole Attack. If neighboring nodes that try to send packets over attacking nodes lose the connection to destination then they may want to discover a route again, broadcasting RREQ messages. Attacking node establishes a route, sending RREP messages. This process goes on until malicious node succeeds its aim (e.g. network resource consumption, battery consumption). This attack is known as routing misbehavior.

1.2.3 Black Hole Attack

In this type of attack, an attacker attempts to prevent legitimate and authorized users from the services offered by the network. A Black Hole Attack can be carried out in many ways. The classic way is to flood packets in the network so that services provided be intermediate node is no longer available to other participating nodes in the network, as a result of which the network no longer operating in the manner it was designed to operate. This may lead to a failure in the delivery of guaranteed services to the end users. Due to the unique characteristics of 5-Gs, there exist many more ways to launch a Black Hole Attack in such a network. Black Hole Attack attacks can be launched against any layer in the network protocol stack [10]. On the physical and MAC layers, an attacker could employ jamming signals which disrupt the on-going transmissions on the wireless channel. On the network layer, an attacker could take part in the routing process and exploit the routing protocol to disrupt the normal functioning of the network. For example, an adversary node could participate in a session but simply drop a certain number of packets, which may lead to degradation in the Quality of Service being offered by the network. On the higher layers, an attacker could bring down critical services by Low Rate Black Hole Attack. Some of the Black Hole Attack attacks are described below:

1.2.4 Jamming

In this form of attack, the attacker initially keeps monitoring the wireless medium in order to determine the frequency at which the destination node is receiving signals from the sender. It then transmits signals on that frequency so that error-free reception at the receiver is hindered. Frequency hopping spread spectrum (FHSS) and direct sequence spread spectrum (DSSS) are two commonly used techniques that overcome jamming attack.

1.2.5 SYN flooding

In this form of attack, a malicious node sends a large amount of SYN packets to a victim node, spoofing the return addresses of the SYN packets. The SYNACK packets are sent out from the victim right after it receives the SYN packets from the attacker and then the victim waits for the response of ACK packet. Without any response of ACK packets, the half-open data structure remains in the victim node. If the victim node stores these half-opened connections in a fixed-size table while it awaits the acknowledgement of the three-way handshake, all of these pending
Connections could overflow the buffer, and the victim node would not be able to accept any other legitimate attempts to open a connection. Normally there is a timeout associated with a pending connection, so the half-open connections will eventually expire and the victim node will recover. However, malicious nodes can simply continue sending packets that request new connections faster than the expiration of pending connections.

1.3 SECURE ROUTING

The routing protocols with in ad hoc networks are more vulnerable to attacks as each device acts as a relay. Any tampering with the routing information can be compromise the whole network. An attacker can introduce rogue information within routing information or replay old logged or stored information.

The aim is to protect any information or behaviour that can update or cause a change to the routing tables on cooperating nodes involved in an ad hoc routing protocol. For completeness, timeliness and ordering are added to the list of desirable security properties that can eliminate or reduce the threat of attacks against routing protocols.

- **Privacy/confidentiality:** Ensuring that no one can read the message except the intended receiver.
- **Integrity:** Assuring the receiver that the received message has not been altered in any way from the original.
- **Non-repudiation*:*** A mechanism to prove that the sender really sent this message.

1.4 ARCHITECTURE OF THE 5-G MOBILE NETWORK

The 5-G network consists of to tier architecture such that in which there is base station and relay
node and mobile device. It is the communication between two or more devices for the
communication.

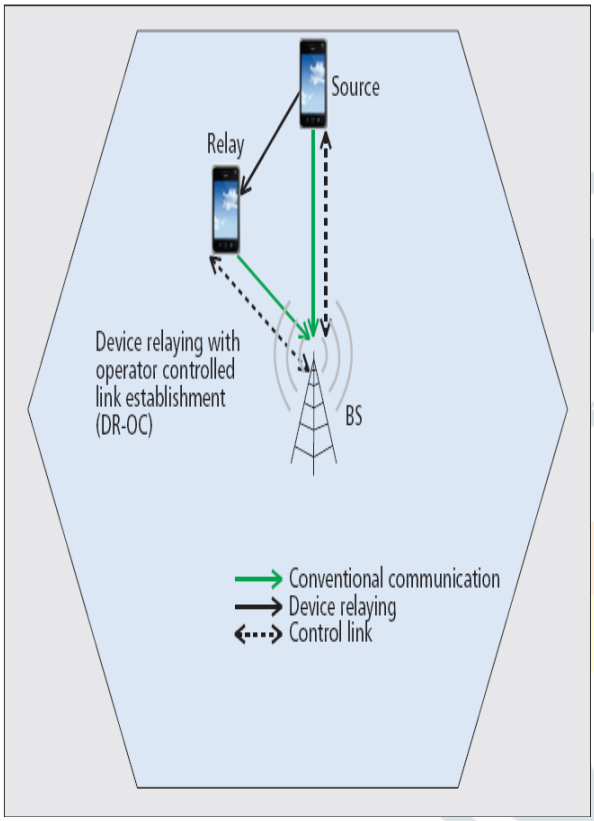

Fig. 1 Architecture of LTE network[1]

II. LITERATURE SURVEY

[1]Yong Niu et al(2015): with the explosive growth of mobile data demand, the fifth generation (5G) mobile network would exploit the enormous amount of spectrum in the millimeter wave (mmWave) bands to greatly increase communication capacity. There are fundamental differences between mm Wave communications and existing other communication systems, in terms of high propagation loss, directivity, and sensitivity to blockage. These characteristics of mmWave communications pose several challenges to fully exploit the potential of mmWave communications, including integrated circuits and system design, interference management, spatial reuse, anti-blockage, and dynamics control. To address these challenges, they carry out a survey of existing solutions and standards, and propose design guidelines in architectures and protocols for mmWave communications.

[2] PimmyGandotra et al(2015):A constant need to increase the network capacity for meeting the growing demands of the subscribers has led to the evolution of cellular communication networks from the first generation (1G) to the fifth generation (5G) . There will be billions of connected devices in the near future. Such a large number of connections are expected to be heterogeneous in nature, demanding higher data rates, lesser delays , enhanced system capacity and superior throughput. The available spectrum resources are limited and need to be flexibly used by the mobile network operators (MNOs) to cope with the rising demands. An emerging facilitator of the upcoming high data rate demanding next generation networks (NGNs) is device – to - device (D2D) communication.

[3] Geordie George et. al(2015): This paper presents a framework that enables characterizing analytically the spectral efficiency achievable by D2D (device-to-device) communication integrated with a cellular network. This framework is based on a stochastic geometry formulation with a novel approach to the modeling of interference and with the added possibility of incorporating exclusion regions to protect cellular receivers from excessive interference from active D2D transmitters.

[4] Sami Hakola et. al(2010): In a cellular network system one way to increase its capacity is to allow direct communication between closely located user devices when they are communicating with each other instead of conveying data from one device to the other via the radio and core network. The problem is then when the network shall assign direct communication mode and when not. In previous works the decision has been done individually per communicating device pair not taking into account other devices and the current state of the network. The system equations capture information of the network such as link gains, noise levels, signal to-interference-and-noise-ratios, etc., as well as communication mode selection for the devices.

[5] Georgios Katsinis et. al(2017): In this paper, the problem of interference mitigation in a multicell Device to Device (D2D) underlay cellular network is addressed. In this type of network architectures, cellular users and D2D users share common Resource Blocks (RBs). Though such paradigms allow potential increase in the number of supported users, the latter comes at the cost of interference increase that in turn calls for the design of efficient interference mitigation methodologies. To treat this problem efficiently, we propose a two step approach, where the first step concerns the efficient RB allocation to the users and the second one the transmission power allocation. Specifically, the RB allocation problem is formulated as a bilateral symmetric interaction game. This assures the existence of a Nash Equilibrium (NE) point of the game, while a distributed algorithm, which converges to it, is devised. The power allocation problem is formulated as a linear programming problem per RB, and the equivalency between this problem and the total power minimization problem is shown. Finally, the operational effectiveness of the proposed approach is evaluated via numerical simulations, while its superiority against state of the art approaches existing in the recent literature is shown in terms of increased number of supported users, interference reduction and power minimization.

[6] Michael Haus et. al(2016): Device-to-Device (D2D) communication presents a new paradigm in mobile networking to facilitate data exchange between physically proximate devices. The development of D2D is driven by mobile operators to harvest short range communications for improving network performance and supporting proximity-based services. Two fundamental and interrelated aspects of D2D communication, security and privacy, which are essential for the adoption and deployment of D2D. An extensive review of the state of- the-art solutions for enhancing security and privacy in D2D communication. By summarizing the challenges, requirements, and features of different proposals, The primary goal of their work is to equip researchers and developers with a better understanding of the underlying problems and the

potential solutions for D2D security and privacy. To inspire follow-up research,

III. PROPOSED ALGORITHM

A sequential step are being followed for detection of the grayhole in the network. So that the performance of the network should not be downgraded. This type of network is having average throughput is above or equal to the threshold.

Step1 Source using LTE device select that the node to which data is sent is belonging to the same cluster or to different cluster.

Step2 If the node belongs to same cluster then the Wi-Fi type of spectrum will be used to send the data. Else Cellular spectrum will be used for sending the data.

Step3 for using the cellular spectrum data packet will be sent to the cluster head.

Step4 if the cluster head packet forward ratio is below the threshold limit then grayhole is declared. Else no grayhole node in the network.

Step5 if the grayhole is detected then automatic alternative route selection procedure will be started.

Fig. 2 Algorithm

IV. PROPOSED FLOWCHART

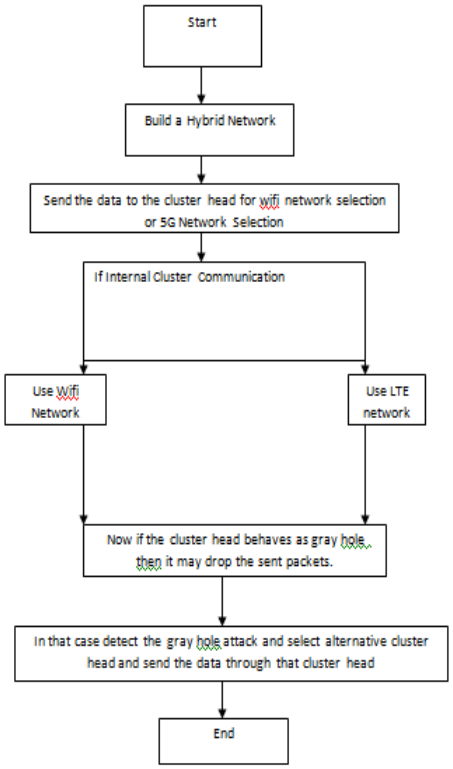

Fig. 3 Flowchart

V. PERFORMANCE PARAMETERS

5.1 Throughput

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

Throughput=Total_Packet_Recieved/Total_Time

5.2 Delay

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

Delay=End_Time-Start_Time

5.3 Packet Delivery Ratio

It is total number of packets delivered to destination against the sent packets.

Packet Delivery Ratio=Packet_Sent/Packet_Received

VI. RESULTS AND ANALYSIS

6.1 NAM Animation

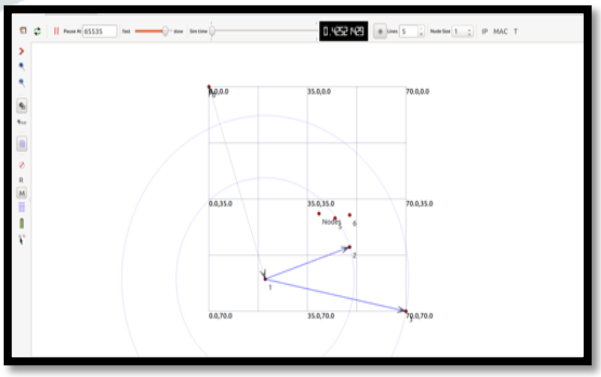

Fig. 4 Nam Animation

6.2 Performance comparison

In current research we have taken three scenarios. One is while network works normal. Second scenario when network is under the attack and third scenario is when there is attacker node has been removed.

Table 1 Parameters

Parameters	Network Before Attack	Network During Attack	Network After Detection and Removal of Attack
Throughput	0.0214109	0.00267636	0.0214109
Packet Delivery Ratio	2	0	2
Delay	983650000.00	983650000.00	1246570000.00

6.3 Comparison for Throughput

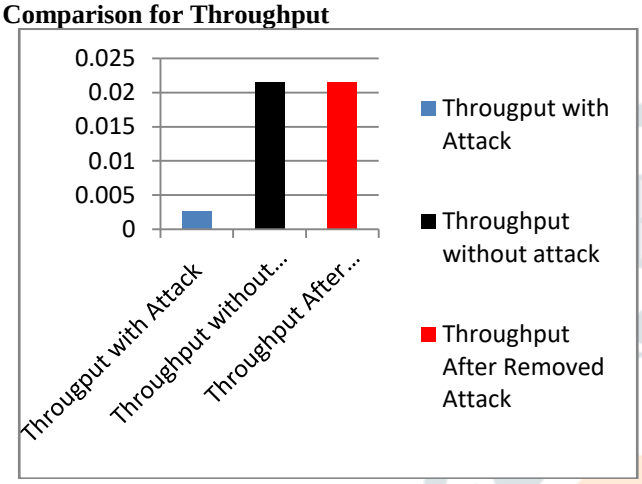

Fig. 5 Throughput comparisons

This graph shows that the throughput has been upgraded or improved after the attacker node has been detected.

6.4 Comparison for Delay

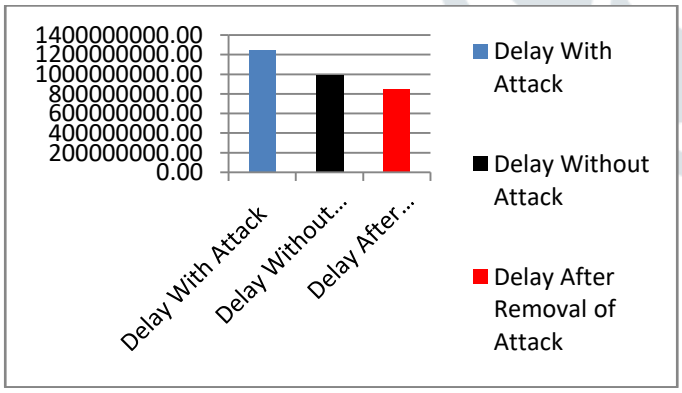

Fig.6 Delay comparison

This graph shows that the delay has substantially be decreased once the attacker node has been detected.

6.5 Comparison for packet delivery ratio

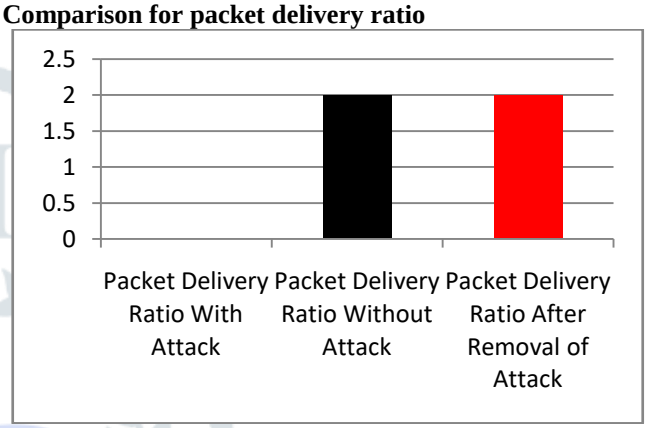

Fig. 7 Packet Delivery Ratio comparison

This graph shows the comparison for packet delivery ratio for network has been improved after the attacker node has been detected.

6.6 Success Rate

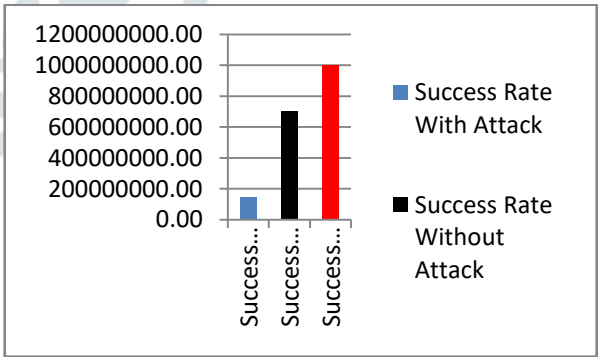

Fig. 8 Success Rate Comparison

This Graph shows the Success rate for network under different scenarios. Success rate has improved after the attacker node has been removed.

6.7 Comparison under Different number of Nodes In the network.

6.7. 1 Comparison of Throughput at 50 Nodes.

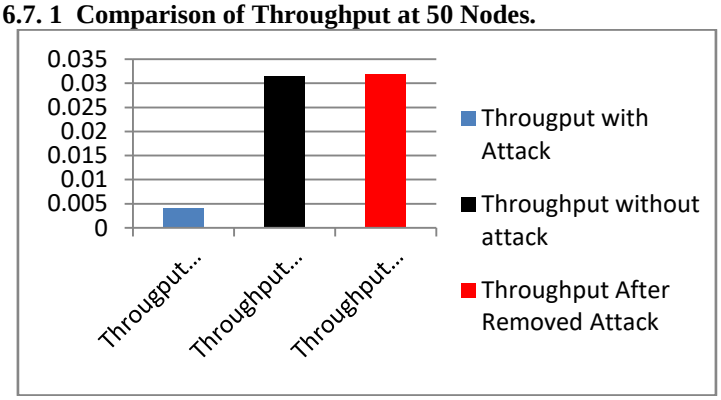

Fig. 9 Throughput

This graph shows the throughput when there are 50 number of nodes. The situation has improved compared to when number of nodes are 15. Because less time will be taken to transfer the data from source node to destination node.

6.7.2 Comparison of Packet Delivery Ratio at 50 Nodes.

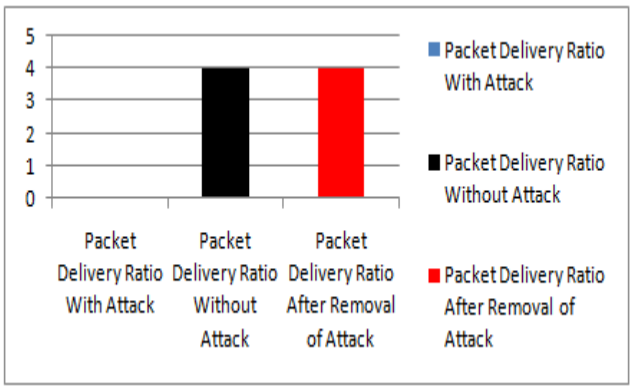

Fig. 10 Packet Delivery Ratio

This graph shows the packet delivery ration under 50 nodes in the network. In this situation the network performance has shown the improvement compared to number of nodes in the network are 15.

6.7.3 Comparison of Delay at 50 Nodes.

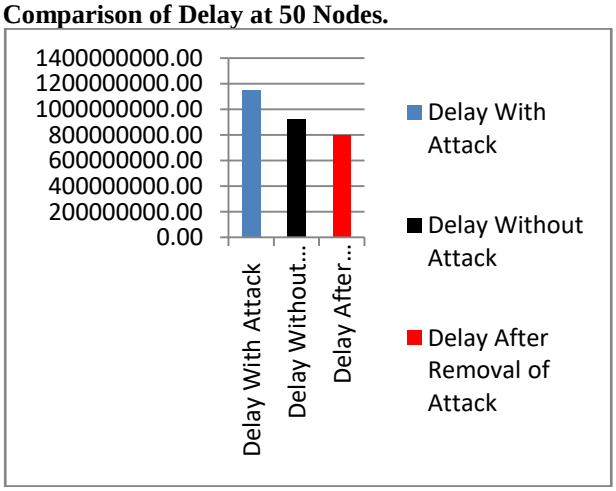

Fig. 10 Delay

This graph shows the delay in the network while communication in the network. This situation has also shown the improvement.

6.7.4 Comparison of Success Rate at 50 Nodes.

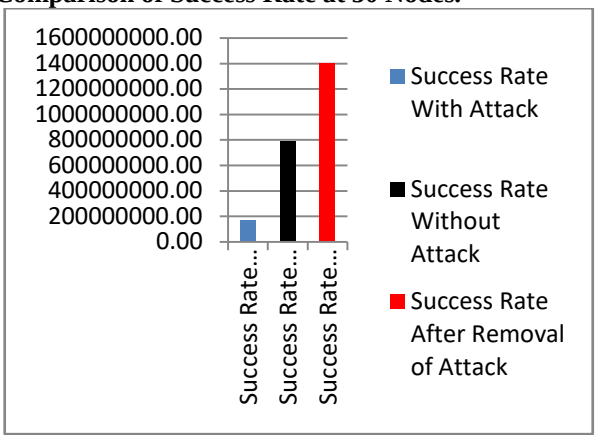

Fig. 11 Success Rate

This graph shows the success rate for the network under different scenarios when number of nodes are 50 in the network.

VII. CONCLUSION

In D2D communication there are various security challenges that can occur due to the network open ended access for both inband and outband services. This type of communication is for efficiency. So that smaller network can be used for larger system with using hybrid type of utility. It is the network layout where large number of system is get through by having proper channelized adaption of user feedback. While there is attack there can be down gradation of the network performance. But the down gradation of the network performance can be checked using proper recovery procedure. So that network performance measuring parameters can be improved.

FUTURE WORK

Current work is based on identification of active attack in the hybrid network. It is the attack performed at the cluster head level. Such that few packets will get dropped rather than being forwarded. But the work can be enhanced by also identifying various passive attacks.

REFERENCES

[1] Zhijian Lin, Zhibin Gao, Lianfen Huang, Chi-Yuan Chen, Han-Chieh Chao,(2015)"Hybrid Architecture Performance Analysis For Device to device Communication In 5G Cellular Network",ElseVier, vol. 20, issue 6, Pp 713–724.

[2] Yong Niu, Yong Li,(2015)" A Survey Of Millimeter Wave (Mmwave) Communications For 5G: Opportunities And Challenges", ElseVier ,vol. 12, issue 4, Pp 345-355.

[3] PimmyGandotra,(2015),"Device-To-Device Communication In Cellular Networks: A Survey", ElseVier ,vol. 2,issue 7,Pp 567-577.

[4] Magri Hicham, NoreddineAbghour And Mohammed Ouzzif,(2016),"DEVICE-TO-DEVICE (D2D) Communication Under LTE-Advanced Networks", International Journal Of Wireless & Mobile Networks (IJWMN) ,Springer,vol. 8,issue 9,Pp 234-240. .

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

[6] Yujae Song, Ki Won Sung,(2016)," Coexistence of Wi-Fi and Cellular With Listen-Before-Talk in Unlicensed Spectrum", ElseVier ,vol. 20,issue 4,Pp 78-86. (Placeholder1)

[7] Geordie George,(2015),” An Analytical Framework for Device-to-Device Communication in Cellular Networks An Analytical Framework for Device-to-Device Communication in Cellular Networks”, ElseVier ,vol. 5,issue 8,Pp 89-97.
[8] Sami Hakola, Tao Chen,(2010),” Device-to-Device (D2D) Communication in Cellular Network - Performance Analysis of Optimum and Practical Communication Mode Selection”, ElseVier,vol. 78,issue 5,Pp 190-200.
[9] Georgios Katsinis, Eirini Eleni Tsiropoulou, SymeonPapavassiliou,(2017),” Multicell Interference Management in Device to Device Underlay Cellular Networks”,ElseVier,vol. 4,issue 6,Pp 890-900.
[10] Michael Haus, Muhammad Waqas, Aaron Yi Ding,(2016),” Security and Privacy in Device-to-Device (D2D) Communication: A Review”, ElseVier,vol. 5,issue 6,Pp 123-130.