IJARSCT

ISSN (Online) 2581-9429

International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)

Impact Factor: 6.252

Volume 2, Issue 2, July 2022

Device-to-Device Communication in 5G Networks

Mr. Nagesh U B[1], Shravani M S[2], Shravya[3], Shreya L[4], Shreyas Moolya[5]

Assistant Professor, Department of Information Science and Engineering[1]

Students, Department of Information Science and Engineering[2,3,4,5]

Alvas Institute of Engineering and Technology, Mijar, Moodbidri, Karnataka, India

Abstract: *Device-to-device communication produces a new dimension in the mobile environment, easing the data exchange process between physically neighboring devices. 5G wireless networks are expected to carry large traffic volumes due to the growth of mobile devices and the increasing demand for high data rates from applications. Device to device communication is one of the suggested technologies to support this increasing load and enhance the capacity of networks. However, the implementation of D2D communication reveals many barriers that include communication scheduling, for which the architecture remains complex and obscure. The mobile operator's action to collect the short-range communications for maintenance of the proximity-based services and improve the performance of networks drives the development of D2D. Through direct communication, device-to- device technology can increase the overall throughput, enhance the coverage, and reduce the power consumption of cellular communications There are popular low- level D2D techniques available for short- range wireless transmissions, such as Bluetooth and WiFi -Direct, and typically they use license-exempt bands. Most of the cellular technologies, however, do not support direct over-the-air communication between end users.*

Keywords: 5G Networks

I. INTRODUCTION

5G networks are expected to be deployed by 2020 and by the year nearly 60 percent of the world's population will be living in urban environments Due to the increasing number of mobile devices in cities, 5G is expected to play an important role in the development of smart city applications 5G offers great promise, potentially giving individuals the opportunity to communicate with whomever they want whenever they want in the context of a "human-centric system" Device-to-device

(D2D) is a radio communication technology that allows devices to directly exchange data without the need for base stations or access points Smart devices are becoming ubiquitous; these devices are supported by all- IP fourth generation LTE networks. The global mobile traffic encountered a growth of around 70%, where 26% of the total global mobile devices were smartphones and were responsible for 88% of the total mobile data traffic. This was the result of the user-oriented mobile multimedia applications such as mobile video conferencing and video streaming. Cisco's Visual Networking Index (VNI) forecasted that smart devices will compose over half of the connected devices to mobile networks by 2019. With this expected increase of smartphone usage and its consequential data traffic, new technologies are needed to address this issue and work on enhancing the network's capacity in terms of supporting a larger number of users, noting that 5G wireless systems are expected to support these technologies while improving data rates and quality of service. New communication technologies must be capable of exchanging data on-demand over proper network connections, and must be able to scale the network capacity. Device-to-device (D2D) communications are considered to be a promising technique that allow mobile devices to communicate with one another directly without going through access points or BSs. There are several studies that have been conducted to analyze the use of D2D in cellular networks. For example, the authors in proposed a machine-learning-based code dissemination (MLCD) scheme to reduce the costs of ground control stations (GCSs) arising from the need to organize vehicles in large quantities as code disseminators. 5G wireless communications envision a significant increase of wireless data rates, bandwidth, coverage and connectivity with a decrease of latency and energy consumption. Considering the network capacity, the traffic volume in 5G networks is predicted to attain tens of Exabytes An extensive survey on issues involving wireless security is given by Zou et al. Security will be of paramount importance in 5G networks, because 5G devices will directly affect our safety in urban environments, such as by controlling self- driving vehicles, traffic lights, utilities, and personalized health care appliances.

DOI: 10.48175/IJARSCT-5842

5G will also be supporting millions of devices that already exist without adequate built-in security, as of smart city applications 5G offers great promise, potentially giving individuals the opportunity to communicate with whomever they want whenever they want.

II. SECURITY AND PRIVACY IN D2D COMMUNICATIONS

To date, many of the standardization and research studies are mainly focused on resource management, interference management and the architecture in D2D communication. Both industry and academia largely ignored the security aspect of the D2D communication environment. D2D communications a hybrid framework where the centralized and the distributed approaches are paired together. That is why it is risky to some of the privacy and security threats that are being identified by both the ad-hoc wireless and the cellular networks. Some of the security threats faced by D2D communications can a act the confidentiality, authenticity, availability, and also integrity of the network. The issue that the authors identify in the 4G and 5G environment is the lack of restriction in the network and the fast- vertical handover, which leads the devices likely to vulnerabilities like privacy, data confidentiality, communication security, access control, and availability. The reason for this is that the devices will be exposed to all the vulnerabilities that are IP-specific since the environment of 5G cellular networks is IP-based security solutions to allow private, secure, and also trusted data exchange among cellular network and devices including direct proximity-based communication without any help from the cellular network. Table 4 shows the overview of security issues and, recently, solutions proposed by the researchers in D2D communications.

In this article, we envision a two-tier 5G cellular network with so-called macro cell and device tiers. The macro cell tier involves base station (BS)-to-device communications as in a conventional cellular system. The device tier involves D2D communications. If a device connects the cellular network through a BS, this device is said to be operating in the macro cell tier. If a device connects directly to another device or realizes its transmission through the assistance of other devices, these devices are said to be in the device tier. In such a system, the BSs will continue to serve the devices as usual. However, at cell edges or congested areas, devices will be allowed to communicate with each other, creating an ad hoc mesh network. In the realization of device-tier communications, the operator might have different levels of control. Based on the business model, it either exercises full/partial control over the resource allocation among source, destination, and relaying devices, or prefers not to have any control. Therefore, we can define the following four main types of device-tier communications (Figs. 1–4): Device relaying with operator controlled link establishment (DR-OC): A device at the edge of a cell or in a poor coverage area can communicate with the BS through relaying its information via other devices. This allows for the device to achieve a higher QoS or more battery life. The operator communicates with the relaying devices for partial or full control link establishment. Direct D2D communication with operator controlled link establishment (DC-OC): The source and destination devices talk and exchange data with each other without the need for a BS, but they are assisted by the operator for link establishment. Device relaying with device controlled link establishment (DR-DC): The operator is not involved in the process of link establishment. Therefore, source and destination devices are responsible for coordinating communication using relays between each other. Direct D2D communication with device controlled link establishment (DC-DC): The source and destination devices have direct communication with each other without any operator control. Therefore, source and destination devices should use the resource in such a way as to ensure limited interference with other devices in the same tier and the macro celltier. A two-tier cellular system, if carefully designed, can bring significant improvements over the classical cellular system architecture. Before the introduction of D2D functionality, several technical challenges, particularly in security and interference management issues, should be overcome. Since the user data is routed through other users' devices, security must be maintained for privacy. One possible solution to ensure security is closed access for the devices that want to operate in the device tier. In closed access, a device has a list of "trusted" devices, and devices not on this list must use the macro cell tier to communicate with it. For example, the users in a neighborhood or workplace that know each other, or the users that have been authenticated via a trusted party such as an organization, can directly communicate with each other, satisfying a level of privacy. The devices in a group can set a proper encryption between each other to avoid divulging their information to other devices. In open access, on the other hand, each device can act as a relay for other devices without any restrictions. Since there is no type of supervision, security in such a case is a challenging open research problem. Security issues in D2D communication involve the identification of potential attacks, threats, and vulnerability of the system. Earlier works on

DOI: 10.48175/IJARSCT-5842

the security issues of machine to-machine communication can be exploited to address security issues in open access D2D. For example, the work in proposes a trusted environment to establish trust relationships among M2M equipment, while secrecy-based access control is discussed. Secure routing, software-based symmetric key cryptography, and detection of potential attacks are further investigated. Another significant concern in a two-tier system is interference management. In DR-OC and DC-OC, resource allocation and call setup are performed by the BS. Therefore, the BS can alleviate the problem of interference management to some extent using centralized methods, a well-established research area in wireless communications. On the other hand, in DR-DC and DC-DC, there is no centralized entity to supervise the resource allocation between devices. Operating in the same licensed band, devices will inevitably impact macro cell users. To ensure minimal impact on the performance of existing macro cell BSs, a two-tier network needs to be designed with smart interference management strategies and appropriate resource allocation schemes. Besides the interference between the macro cell and device tiers, there is also interference among users in the device tier. To address resource allocation for this type of communication, different approaches such as resource pooling, non-cooperative game or bargaining game, admission control and power allocation, cluster partitioning, and relay selection can be employed. In DR-OC, as illustrated, since the BS is one of the communicating parties, some of the aforementioned challenges can be addressed by the control of the BS using existing methods. The BS can authenticate the relaying devices and use the appropriate encryption to maintain sufficient privacy for the information of the devices. The BS can also manage spectrum allocation between the relaying devices to prevent them from interfering with other devices. In DC-OC, the devices communicate directly with each other with operator controlled link establishment. Specifically, the operator deals with access authentication, connection control, resource allocation, and monetary interaction between devices. It has full control over the D2D connections, including control plane functions (e.g., connection setup and maintenance), and data plane functions (e.g., resource allocation).

III. JAMMING

A property of 5G networks is opportunistic spectrum access, which means that secondary users sense spectrum vacancies and utilize that spectrum while not interfering with its primary users (PUs). One side effect is that frequencies are subject to jamming. Jamming is the malicious insertion of noise or signals into a channel in order to prevent the channel's use. Li and Cadeau study both the jamming capabilities of some actors in a cognitive radio network, and the anti-jamming capabilities of others (Li and Cadeau 2011). They identify three jamming strategies. Under strong jamming, a transmission is completely disrupted. To escape strong jamming, sender and receiver must switch to an unjammed channel. Light jamming injects enough interference to make a user assume the interference is caused by a primary user and switch channels. Smart jamming jams only the control signals. Lichtman et al. assess the threat and mitigation of jamming specifically in 5G networks. One 5G property that mitigates jamming is its wide range of frequency use. Specifically, using frequencies greater than 24GHz inhibits jamming, because of the difficulty of building a jammer for cells operating above 24GHz (Lichtman et al. 2018). In 5G networks Primary and Secondary Synchronization Signals (PSS and SSS) are control signals which allow a device to identify base stations with low SINR. This makes them resilient to jamming because it requires an attacker to use "more jamming power to successfully jam the signal". Techniques that spread signals over a wider bandwidth such as direct sequence spread spectrum (DSSS) and frequency hopping spread spectrum (FHSS) are used in 5G networks to act against jamming at the physical layer (Fang et al. 2018). In general, schemes that utilize hopping rely on sharing a key between sending node and receiving node. How this can happen in an open environment with potential jamming is a difficult question, because the key propagation depends on communication, and communication depends on key propagation. This is referred to as the anti-jamming/key- establishment dependency. In Strasser et al. (2008), propose to break this dependency using a scheme called Uncoordinated Frequency Hopping (UFH). In UFH, potential senders and receivers hop along randomly chosen frequency channels, with the sender sending partial messages at each frequency. UFH is especially interesting because it also guards against injecting attacks if each part of the message received contains a hash that points to the next part of the message. An anti-jamming protocol for cognitive radio networks is proposed by Bhattacharya et al. (2016). In this protocol, both sending and receiving nodes share knowledge of randomly-generated sequence of channels, generated based on a shared key. If the receiving node senses that it is jammed, it sends a jammed message to the sending node, which is not jammed and is therefore able to receive it. The receiving node may also detect a collision between the jammed signal and the signal from the sending node, in

DOI: 10.48175/IJARSCT-5842

which case it sends a collision signal. After some pre- agreed number of jammed or collision messages, both parties switch to a new, mutually known channel. If the sender is jammed, it sends move-to-next-channel requests instead of data. The receiver can hear this request, and send an acknowledgement (ACK), which cannot be received by the sender due to jamming. However, after some number of messages are sent during a number of time slots, both parties switch to a new channel, unknown to the jammer. When both are jammed, they perform similarly to the first two cases, and switch channels after a time. Another frequency-based model is proposed by Su et al. (2011). They assert that a weakness of models where new channel assignments are pre known is that a jammer potentially has access to the same information. In their model, both sender and receiver use learning to determine which channel to switch to. Here, both sender and receiver are given a multi-armed bandit (MLB) algorithm. Based on successful outcomes, both parties learn to sense which channel the other will pick.

IV. DISASTER MANAGEMENT USING D2D

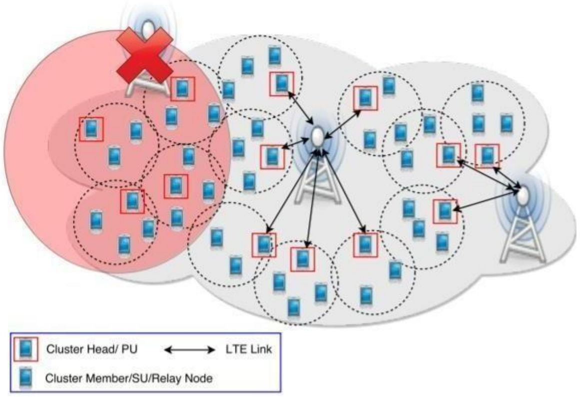

Figure 1 Scenarios of implementing D2D

D2D technology in 5G is not just to make it easier for a few people in the field of communication technology. If examined further, D2D technology on 5G can help the mitigation and evacuation process when natural and non- natural disasters occur. As an illustration, Tsunami disasters and large earthquakes often occur without warning. In Nepal, in 2015 there was a major earthquake that killed at least 8,000 people and injured at least 250,000, and caused the collapse of several historic buildings.

In a disaster, the effective use of radio resources is essential with the aim of serving the affected people to gather information from different sources in the disaster zone. In this context, D2D communication will be effective as for example, D2D based solutions allow efficient spectrum allocation with low latency rates.

The application of this technology in the real world still requires further study and research to be able to solve the problems described above with the hope of creating D2D technology on 5G with maximum performance, low latency, and privacy and security that makes users feel safe and comfortable in using technology.

V. CONCLUSION

Security is an important consideration in 5G networks, and many methods have been proposed to enhance it. It is interesting to observe that these methods differ from defenses against similar attacks on wired and other networks because of the unique properties of wireless and 5G networks. Eavesdropping will be a constant problem due to open architecture and the cooperation of devices. Defenses range from simply moving away from the eavesdropper, to using friendly jamming to confuse it. Jamming limits the access of users to limited bandwidth resources. Again movement is a suggested defense, however this time it is the movement of the transmission to different channels, hopefully in a pattern that a jammer will be unable to detect. The primary user emulation attack is a form of denial-of-service attack to which 5G networks are particularly susceptible. Defenses against this type of attack involve determining the location of primary users in order to distinguish them from emulators. This can be done individually, through a dedicated sensor network, or through a group of devices using a non-centralized strategy. Last is the injecting attack, against which cryptography and authentication are often mentioned as defenses. We have presented a comprehensive survey of the literature on these four types of attacks. In response to eavesdropping specifically, we have considered the defense strategy of multipath routing and the security implications related to it. Related works on multi path routing were presented, along with a simulation that tested three different method of choosing the paths. It was found that strategies that choose interference-disjoint paths work best to prevent eavesdropping. It was also found that, while increasing the broadcast radius of mobile devices increases potential eavesdropping, increasing the density of nodes mitigates the problem by providing additional possible paths.

REFERENCES

[1]. Osseiran, A., Boccardi, F., Braun, V., Kusume, K., Marsch, P., Maternia, M., Queseth, O., Schellmann, M., Schotten, H., Taoka, H., Tullberg, H., Uusitalo, M. A., Timus, B., and Fallgren, M., "Scenarios for 5G mobile and wireless communications: The vision of the METIS Project," IEEE Communications Magazine, vol. 52, no. 5, pp. 26–35, May 2014.Google Scholar

[2]. Muthanna, P. Masek, J. Hosek, R. Fujdiak, O. Hussein, A. Paramonov, and A. Koucheryavy, Analytical Evaluation of D2D Connectivity Potential in 5G Wireless Systems,Lecture Notes in Computer Science Internet of Things, Smart Spaces, and Next Generation Networks and Systems, pp. 395– 403, 2016.

DOI: 10.48175/IJARSCT-5842