iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 11 **Issue:** X **Month of publication:** October 2023

DOI: https://doi.org/10.22214/ijraset.2023.56159

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 11 Issue X Oct 2023- Available at www.ijraset.com

Survey on 5G Security Challenges in Device to Device Communication

Amul[1], Dr. Prashant Kumar[2]
[1]*Department of Computer Science, Dr B R Ambedkar National Institute of Technology, Jalandhar*
[2]*Assistant Professor, Department of Computer Science, Dr B R Ambedkar National Institute of Technology, Jalandhar*

Abstract: ***Mobile communication networks have evolved from first generation to fifth generation as a result of a continuing requirement for enhancing network's capacity to satisfy the expanding needs of customers (5G). In following years, the no. of linked devices is estimated to grow to over fifty billion, according to estimates.***
The heterogeneity of such a vast number of connections is expected, necessitating faster data rates, shorter latency, more system capacity, and higher throughput.
Mobile networks will have to be expanded to meet up with increasing expectations. In order to meet consumers' expanding expectations and make efficient use of limited sources, D2D communication is regarded as an innovative technique for existing and future wireless networks.
It permits users to connect with one another, resulting in increased energy efficiency and system throughput. This study provides a thorough examination of D2D communications, as well as the security challenges that D2D must address in order to become a viable wireless network paradigm.
Keywords: Mobile network operators (MNOs), Device-to-device communication, Security, Next generation networks (NGNs)

I. INTRODUCTION

Existing wireless network technologies are frequently insufficient to keep up with the growing demands of customers. The popularity of a number of high-bandwidth platforms, such as mobile computing and video streaming, has contributed to this surge in usage. By 2020, billions of people will be served by trillions of wireless devices [1].

Due to the overpopulation of the spectrum, new strategies for more efficient use of spectral resources are being researched [2]. The concept of 5G wireless networks is basically an amalgamation of a variety of technologies being extensively investigated. These networks are primarily supporting the new usage situations. D2D Communication is an effective approaches for achieving the technological goals of next-generation networks.

Data is delivered directly from one device to another without transmitting via a base station in D2D communication. Spectrum efficiency, system capacity, and latency of this sort of direct transmission are all improved [3]. It enables cell carriers to offer location-based services.

Despite the fact that D2D communication was disregarded throughout the 1G, 2G, 3G, and 4G wireless connections, telecom corporations are increasingly interested in D2D technologies as time passes [4]. It gives a cost-effective offloading option for wireless network providers.

WPANs and WLANs were traditionally utilised for lesser energy directly transmission and reception. These techniques work in license exempted spectrum, enabling for low-cost local services.

D2D connectivity could be linked to various technologies such as mobile cloud services, mobile data unloading, crisis response, and so on. Figure 1 depicts an useful reference of D2D communication in cellular channels. The diagram illustrates diverse use cases in individual cells, only with base station inside the central core.

The figure illustrates vehicle to vehicle communication well with Internet of Vehicles, public health and safety assistance, offload of cellular traffic from BS and so on.

In 5G technology, Cloud Radio Access Network allows for more adaptable system design. It centralizes network functionality according to the software being served. Smaller units, in combination with D2D transmission, could be an efficient tactic of boosting range and allowing traffic unloading for 5G mobile networks and even beyond.

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 11 Issue X Oct 2023- Available at www.ijraset.com

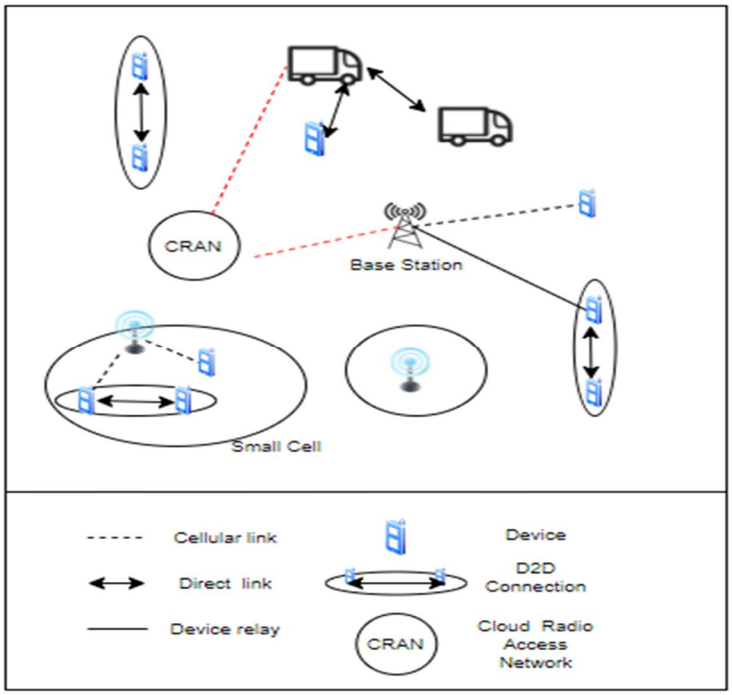


Fig 1: A general D2D scenario

D2D connectivity allows for directly wireless communication, greatly expanding spectrum utilisation. The licenced band surpasses the unlicensed spectrum when it comes to interfering since involvement can be handled because of central governing object present in licenced spectrum i.e. Evolved NodeB. When unmanageable interference levels occur, quality of service degrades, which is undesirable. Apart from unacceptable interfering rates in licence exempted bands, conventional direct transmission techniques absorb extra energy and cause battery difficulties. Device to device communication is thus a viable solution for direct transmission in regulated environment, resulting in improved network throughput [5].

It allows for establishing connections among nearby objects and increases network speed, but it has a number of disadvantages. To establish direct links, users must first find each other. The process of discovery is currently being followed in depth. On the mobile network, there seems to be a significant risk of disruption among D2D and cellular users. In order to communicate via direct links, D2D users must have access to resources. Positioning of relays in D2D situation can extend the transmission range. Due to the vulnerability of relays and other connecting devices to distinct assaults, guaranteeing security in D2D communication is crucial. All of these concerns necessitate additional attention [5].

As a consequence, it's vital to stress the potential threats that arise not only as an outcome of cellular networks' wireless characteristics, but even in future developments which will be extremely crucial for 5G. In this article, we discuss the essential security challenges which are at the frontline of 5G and that necessitate rapid security measures. The rest of the paper is organised as follows: Section II discusses security considerations, while Section III discusses security challenges. Section IV brings the paper to a close.

II. SECURITY ISSUES FOR 5G NETWORK

The user is identified, authorised, and then the broadcasting link is encrypted in standard cellular transmission. The core network is a trustworthy source of data. However, with D2D communication, this isn't true since transmissions takes place alone without help of the core site. [24]. In natural world, wireless channels are also disseminated. As a result, they're subject to a wide range of dangers, necessitating a high level of security. Cryptographic procedures are required to keep data secure as it travels across wireless networks [25].

D2D users can employ the safety techniques given by cellular operators if they are inside their coverage area. Consumers outside of the providers' reach, on the other hand, are unprotected. Security signals could be sent through relays in this instance [26]. Relays are renowned for being vulnerable to malicious assaults, building security methods for D2D communication is a major undertaking. [27] discusses security considerations in device to device communication.

Device to device receivers must address any perceived dangers owing to the mobile communication environment because the eNB only serves as a regulator in D2D connections. Device - to - device subscribers' impulses are digitally spread in a certain zone, and if an attacker is inside that scope, this will receive crucial data [28]. Second, units are meant to offload signals from the enodeb, simplifying the unit but rendering it incapable of verifying associated devices. Furthermore, these authentication activities consume a lot of equipment processing power.

Furthermore, due to the improved spectral efficiency of Device to Device communication in underlay manner, routes are pooled with mobile network, posing a direct threat to both broadband and Mobile users. As a consequence, researchers are forced to concentrate on Device-to-device secure communication. According to 3GPP [5], the LTE system has five tiers of security:

1) The safety of network access
2) Domain security on the network
3) Domain security for users
4) Domain security for applications
5) Security visibility and configuration.

There are three dimensions to the security model. visually 1) Are you an insider or a stranger? 2) Are you passive or active? 3) restricted or unrestricted [9]. Internal intruders are network invaders who have been authenticated, wherein externals are unlawful attackers. Local intruders are invaders who have a restricted impact on devices, whereas extended attackers corrupt things across large networks. Because a passive attack don't harm system, it is tough to identify because network functionality is unaffected. Active attacks disrupt communication by destroying or altering data sent in the network. The following diagram depicts multiple attacks on the layers:

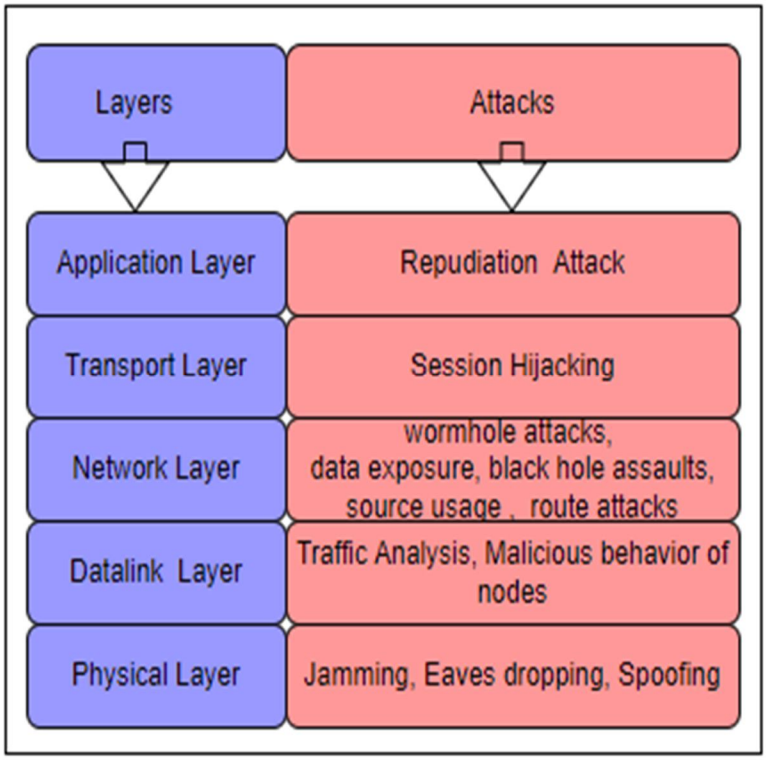


Fig 2: Various attacks on distinct layers

a) Network layer attacks include wormhole attacks, data exposure, black hole assaults, source usage and route attacks.
b) Session hijacking at the transport layer. Once the authenticated session is created, the intruder acts as one of the nodes and hijacks the data.
c) Repudiation occurs at the application layer. In a repudiation attack, a communication node refuses to communicate.
d) Data link Layer includes Traffic Analysis, Malicious behavior of nodes.
e) Other attacks include denial of services, impersonating, internet traffic manipulations, and man in the middle.

A. Standards for Security

In terms of D2D communication, the devices must meet the following security requirements [8]:

1) *Confidentiality:* Data and control signals from D2D users must only be shared with authorised users. In relay modalities or team communication usage scenarios, control and data streams are protected from outsiders, ensuring their confidentiality.
2) *Message Integrity:* Message integrity is crucial in relay means of communication, where a device transmits data to a recipient. False messages are inserted by malicious nodes into the transmitted data, resulting in data integrity loss. Frames injecting, information replaying, and authenticity replay are all threats which induce integrity compromise [10].
3) *Secure routing:* Control and data streams must be protected from tampering in relaying mode because they pass via more than two nodes.
4) *Authentication:* In D2D communication, devices communicate without the need for a central authority. Devices to validate legitimate receivers or senders before commencing data transfer are required in the absence of a governing authority.
5) *Authorization:* Once the authentic user has been determined, D2Ddevices must grant other users full, partial, or limited access. To safeguard D2D communication from impersonation attacks, authorization is required.
6) *Non-repudiation:* Once a device has been allowed, it cannot afterwards refute its ability to utilize the network. However, the non-repudiation requirement makes approved devices a network threat. . Some devices, once authorized, may refuse to allow their resources to be used, resulting in the exposure of hidden information.
7) *Availability:* Often in the presence of denial of services assault or jammer attack, systems must be able to interact for D2D communication to work. Otherwise, D2D communication's sole goal of offloading traffic will remain unaddressed.
8) *Revocability:* Its important to conradict authorization given to subscribers later discovered to be harmful.

B. Metrics for Secrecy

For assessing the safety of device to Device communication, several secrecy techniques have been suggested [11].

1) *Secrecy Capacity:* It's fastest rate upon which secret data can be transmitted from sender to recipient when eavesdroppers are present.
2) *Probability of a Secrecy Outage:* This is chance that instant capacity exceeds duplicacy rate. The difference between transmission rate and secrecy rate is redundancy rate.
3) *Secrecy Energy Efficiency:* The ratio of secrecy capacity to total power consumption is known as secrecy energy efficiency.
4) *Secrecy Rate:* The discrepancy in between highest rate of significant communication link and highest rate of eavesdropper.
5) *Secrecy Throughput:* A Device to device recipient's average amount of confidential information collected every unit of time is described as this.

III. IMPLEMENTATION CHALLENGES IN D2D COMMUNICATION

Device discovery, which requires devices to advertise their location to the network, initiates D2D communication. The pairing step follows device detection and is based upon nearest position and optimal channel situation. Choosing modes, allocating sources and communicating are the next steps in the process. Although D2D communication at the cell edge regions delivers lower latency, faster information rates and lesser outage likelihood conditions, there are some flaws that must be solved. Lower operational capacity, object's energy constraint and shared link are some of the ambiguities [5].

Mobile communication through the air interface is protected by network access security. A safe network requires authentication, privacy, cryptography, and message integrity. The goal of network domain security is to ensure that data and control signals are exchanged securely between network nodes. Network domain security is enabled via privacy at radio accessing system. The goal of user domain security is to provide safe access to mobile devices. Safe accessing among apps and subscribers and servers is provided by application level security. Visibility and configuration security enable availability and security level configurations. These degrees of security protect the network and its users from numerous vulnerabilities and threats. [33] looks into the incredible potential of device to device communication in the IoT for next-generation networks.

[29] look into physical layer safety to improve system's secrecy capabilities. Enabling D2D communication in cellular networks improves efficiency, power usage, and other variables. Despite the concern that this topic needs extensive research, security problems are rarely addressed. An attacker can capture crucial data by exploiting the core network or user apps, impeding information exchange through direct routes. Physical layer protection is necessary for D2D communication to be safe. The term "physical layer security" was coined to study the actual characteristics of cellular connections. An eavesdropper in a communication network may be able to collect sensitive information. Physical layer security uses techniques that take advantage of the wireless channel's properties, such as modulations, codings and various antennas to prevent attacks like eaves dropping etc.

The authors investigate physical layer safety in cooperative D2D networks in [30]. Users of cellular and D2D create a coalition to work together. When D2D communication is integrated with IoT and various connected devices [31] is created that may be used for a variety of purposes. In the IoT, [32] explores how to develop intelligent D2D connection. It uses least amount of energy, making the Internet of Things more energy efficient (IoT).

Vehicular interaction is a unique implementation discovered in vehicle crashes alert system [34], brake collaborating mechanisms, and advanced driver assistance systems [35]. D2D services have the potential to become a crucial element of public protection and disaster relief (PPDR) and national security and public safety (NSPS) solutions [36]. Authors investigated the need for a connectivity to assist them. D2d is thus an increasingly prominent innovation in the field [37]. Table 1 summarizes the challenges encountered in these three key topics.

Table 1
Security challenges faced in D2D communication

Latency	When it comes to essential processing, latency rises.
Computational Complexity	The use of modern security methods increases the computational complexity of the system.
Relay mode	The usage of relay mode for better spectral and energy efficiency creates a security hazard that necessitates a balance.
Physical layer	The identification and use of physical layer characteristics for security purposes may cause interference.
IDS	The addition of IDS to the DUE adds to the device's complexity.
Beamforming	Because CSI knowledge is required, but eavesdropper knowledge is not, various models are used, lowering the attained secrecy rate.

The relays, base stations, and tiny cell access points of wireless link are all prone to Hacking in 5G network. For such elements, [13] developed an adaptable IDS based on game theorrtic and a Nash equilibrium formulated solution. To create an Intrusion Detection System, ML algorithms including active learning SVM classifier, ensemble classification and C-mean grouping can be used. [14] proposes using IDS and an ensemble classification algorithm for machine learning to create intrusion warnings. The RSA technique is suited for IDS on a MANET. Key is generated and RSA process requires encoding and decoding, which increases transmit power due to extra confirmation inside the connection [15]. A contrast of researches on privacy in D2D communication is shown in Table 2.

Table 2
Security in D2D communication

Reference no.	Approach used	Attacks addressed	Requirements fulfilled
Tata et al., [16]	Data splitting, shuffling and coding multipath routing	Session Hijacking	Confidentiality
Shen et al., [17]	Diffie-Hellman parameters	Man In the Middle (MITM)	Confidentiality Authentication
Sedidi et al., [18]	Diffie-Hellman based key exchange	MITM, Brute force Attack	Confidentiality Authentication
Wang et al., [12]	A non-interfering strategy where process of communication has a bad performance warranty.	Information Disclosure	Confidentiality
Sun et al., [20]	Constellation rotation for interference avoidance scheme	Information Disclosure	Integrity, Confidentiality
Cai et al., [19]	To enhance the secrecy performance, physical channel safety is improved by assigning energy to D2D and wireless communication systems.	Session Hijacking	Availability
Chu et al., [7]	With energy and data transfer, BS acts as jamming to an eavesdropping attack.	Denial of Service	Availability
Jiang et al., [6]	SWIPT includes secured beamforming to boost D2D and wireless pair secrecy rates, and energy saving to idle D2D nodes	Information leakage	Confidentiality, Integrity Authentication, Availability Secure Routing
Jayasinghe et al., [13]	For broadcasting and multiple access, safe beamforming utilizing MIMO and physical layer network coding is used.	Information leakage	Secure Routing
Abualhaol et al.,[23]	Legitimacy pattern introduction in the signal, measuring performance by security scoring.	Eavesdropping, jaming, restricting access, injection	Authentication Integrity
Kang et al., [22]	Distributed accessibility to a D2D pair's decision with a high rate of secrecy	Information disclosure	Confidentiality

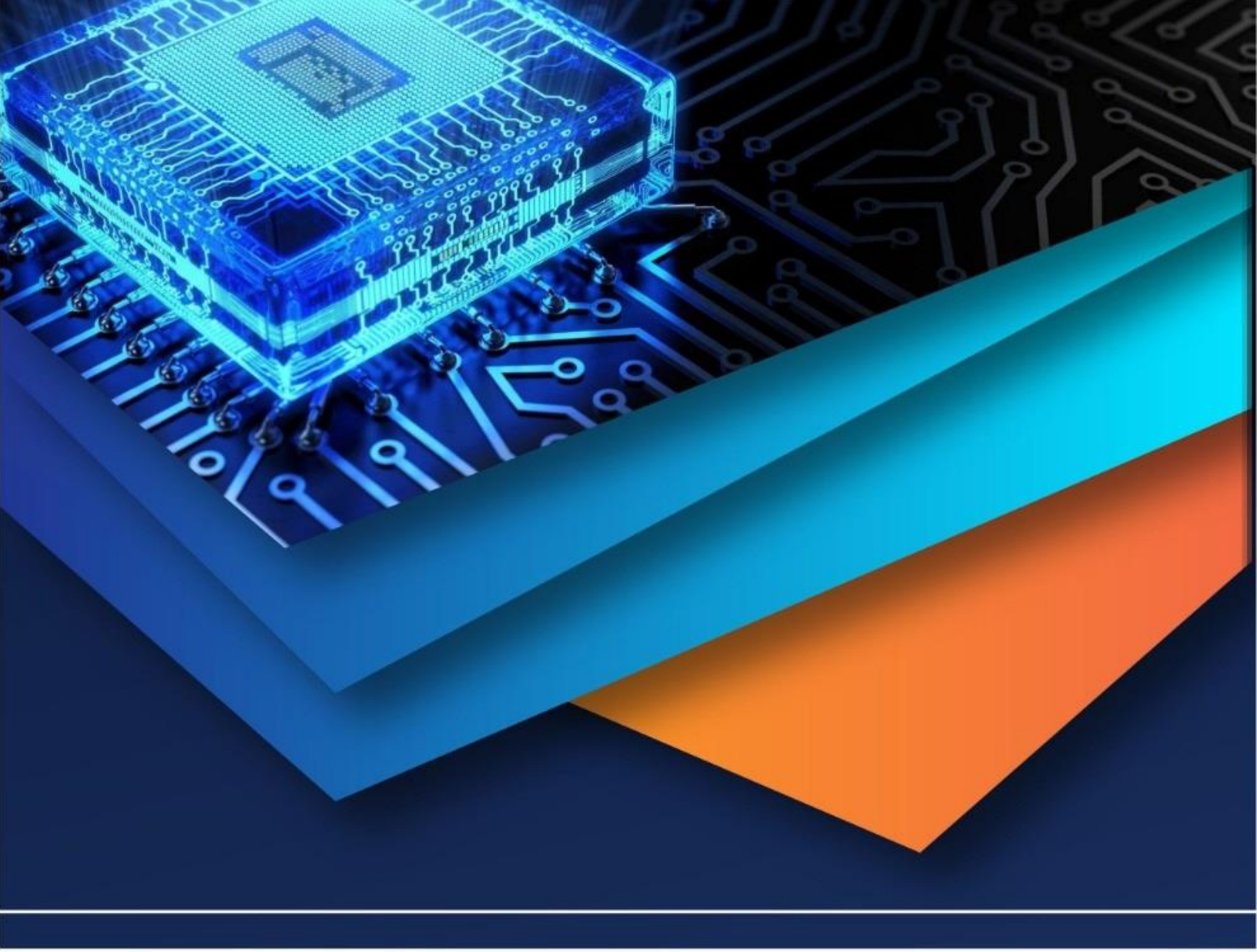
IV. CONCLUSION

In this study, the topic of D2D communication was thoroughly examined. It's a possible next-generation communication system that promises enhanced system capacity, higher throughput, lower latency and better spectrum utilization. Several key components of D2D communication were discussed. With all of their advantages, these technologies also come with security risks. Security threats to D2D communication have been described. As a result, in this paper, we've highlighted the primary security concerns that, if not addressed effectively, could become more dangerous in 5G. There have been a few scenarios in which D2D communication is crucial. Likewise, as more consumer devices, including IoT, are linked and more diverse set of offerings are provided in 5G, data protection issues will be more apparent. To summarise, it is quite likely that when new 5G technology and services are deployed, new forms of security threats and issues will emerge. Consequently, Device to device communication is a key technology for future networks, prompting academics to work out the issues that come with it in order to fully realise its potential. Handling these concerns from the beginning of the design phase through implementation reduces the chance of privacy and security breaches.

REFERENCES

[1] Doppler, Klaus, Cássio B. Ribeiro, and Jarkko Kneckt. "Advances in D2D communications: Energy efficient service and device discovery radio."Wireless Communication, Vehicular Technology, Information Theory and Aerospace & Electronic Systems Technology (Wireless VITAE), 2011 2nd International Conference on. IEEE, 2011.
[2] Hu, Rose, and Yi Qian. "An energy efficient and spectrum efficient wireless heterogeneous network framework for 5G systems." Communications Magazine, 94-101, IEEE 52.5 (2014).
[3] Chai, Yingqi, Qinghe Du, and Pinyi Ren. "Partial time-frequency resource allocation for device-to-device communications underlaying cellular networks." Communications (ICC), 2013 IEEE International Conference on. IEEE, 2013.
[4] D. Astely et al., “LTE Release 12 and Beyond.” IEEE Commun. Mag., vol.51, no. 7, pp. 154-60, 2013.
[5] Pimmy Gandotra, Rakesh Kumar Jha and Sanjeev Jain, “A Survey on Device-to-Device (D2D) Communication: Architecture and Security Issues”, Journal of Network and Computer Applications, 2016
[6] L. Jiang, H. Tian, “Secure beamforming in cooperative d2d communications with simultaneous wireless information and power transfer,” 2016 IEEE/CIC International Conference on Communication in China ,Chengdu, 2016, pp. 1-6
[7] Z. Chu et al., "Game theory based secure wireless powered D2D communications with cooperative jamming," 2017 Wireless Days, Porto, 2017, pp. 95-98.
[8] M. R. Garey and D. S. Johnson, Computers and Intractability: A Guide to the Theory of NP-Completeness, W. H. Freeman and Co., 1979
[9] T. Koskela, S. Hakola, T. Chen, and J. Lehtomaki, “Clustering concept using device-to-device communication in cellular system,” in Proc. IEEE Wireless Communications and Networking Conference, 2010.
[10] S. Hakola, T. Chen, J. Lehtom¨aki andki, and T. Koskela, “Device-todevice (D2D) communication in cellular network–performance analysis of optimum and practical communication mode selection,” in Proc. IEEE Wireless Communications and Networking Conference, 2010
[11] V. Chandrasekhar and Z. She, “Optimal uplink power control in two cell systems with rise-over-thermal constraints,” IEEE Commun. Let., vol. 12, no. 3,Mar. 2008.
[12] C. Ma, J. Liu, X. Tian, H. Yu, Y. Cui and X. Wang, "Interference Exploitation in D2D-Enabled Cellular Networks: A Secrecy Perspective," in IEEE Transactions on Communications, vol. 63, no. 1, pp. 229-242, Jan. 2015.
[13] K. Jayasinghe, P. Jayasinghe, N. Rajatheva and M. Latva-aho, "Physical layer security for relay assisted MIMO D2D communication," 2015 IEEE International Conference on Communication Workshop (ICCW), London, 2015, pp. 651-656.
[14] Xing, Weijun, et al. "Resource allocation schemes for D2D communication used in VANETs." 2014 IEEE 80th Vehicular Technology Conference (VTC2014-Fall). IEEE, 2014.
[15] Ciou, Si-An, et al. "Multi-sharing resource allocation for device-to-device communication underlaying 5G mobile networks." Personal, Indoor, and Mobile Radio Communications (PIMRC), 2015 IEEE 26th Annual International Symposium on. IEEE, 2015.
[16] C. Tata and M. Kadoch, "Secure Multipath Routing Algorithm for Device-to-Device Communications for Public Safety over LTE Heterogeneous Networks," 2015 3rd International Conference on Future Internet of Things and Cloud, Rome, 2015, pp. 212-217
[17] W. Shen, W. Hong, X. Cao, B. Yin, D. M. Shila and Y. Cheng, "Secure key establishment for Device-to-Device communications," 2014 IEEE Global Communications Conference, Austin, TX, 2014, pp. 336-340.
[18] R. Sedidi and A. Kumar, "Key exchange protocols for secure Device-to- Device (D2D) communication in 5G," 2016 Wireless Days (WD), Toulouse, 2016, pp. 1-6.
[19] J. Qu, Y. Cai and S. Xu, "Power allocation in a secure-aware device-to-device communication underlaying cellular network," 2016 8th International Conference on Wireless Communications & Signal Processing (WCSP), Yangzhou, 2016, pp. 1-5.
[20] L. Sun, Q. Du, P. Ren and Y. Wang, "Two Birds With One Stone: Towards Secure and Interference-Free D2D Transmissions via Constellation Rotation," in IEEE Transactions on Vehicular Technology, vol. 65, no. 10, pp. 8767-8774, Oct. 2016.
[21] X. Kang, X. Ji, K. Huang and Z. Zhong, "Secure D2D Communication Underlying Cellular Networks: Artificial Noise Assisted," 2016 IEEE 84th Vehicular Technology Conference (VTC-Fall), Montreal, QC, 2016, pp. 1-5.
[22] X. Kang, X. Ji, K. Huang and X. Li, "Security-oriented distributed access selection for D2D underlaying cellular networks," in Electronics Letters, vol. 53, no. 1, pp. 32-34, 1 5 2017.
[23] I. Abualhaol and S. Muegge, "Securing D2D Wireless Links by Continuous Authenticity with Legitimacy Patterns," 2016 49th Hawaii International Conference on System Sciences (HICSS), Koloa, HI, 2016,pp. 5763-5771.
[24] Cha, Inhyok, et al. "Trust in M2M communication." Vehicular Technology Magazine, IEEE 4.3 (2009): 69-75.

[25] Yue, Jianting, et al. "Secrecy-based access control for device-to-device communication underlaying cellular networks." Communications Letters, IEEE 17.11 (2013): 2068-2071.
[26] Perrig, Adrian, John Stankovic, and David Wagner. "Security in wireless sensor networks." Communications of the ACM 47.6 (2004): 53-57.
[27] Zhou, Yun, Yuguang Fang, and Yanchao Zhang. "Securing wireless sensor networks: a survey." Communications Surveys & Tutorials, IEEE 10.3 (2008):6-28
[28] Muraleedharan, Rajani, and Lisa A. Osadciw. "Jamming attack detection and countermeasures in wireless sensor network using ant system." Defense and Security Symposium. International Society for Optics and Photonics, 2006.
[29] Zhang, Rongqing, Xiang Cheng, and Liuqing Yang. "Joint power and access control for physical layer security in D2D communications underlaying cellular networks." Communications (ICC),IEEE International Conference on. IEEE, 2016.
[30] Zhang, Rongqing, Xiang Cheng, and Liuqing Yang. "Cooperation via Spectrum Sharing for Physical Layer Security in Device-to-Device Communications Underlaying Cellular Networks." 2015 IEEE Global Communications Conference(GLOBECOM). IEEE, 2015.
[31] Bello, Oladipupo, and Sherali Zeadally. "Intelligent Device-to-Device communication in the internet of things.", IEEE Systems Journal (2014).
[32] Bello, Oladayo, and Sherali Zeadally. "Intelligent Device-to-Device communication in the Internet of Things.", IEEE Systems Journal, Vol 10, (2016).
[33] Militano, L., et al. "Device-to-Device Communications for 5G Internet of Things."IOT, EAI, (2015).
[34] Hayami et.al. “Crash warning for intersection and head-on car collision in vehicle –to-vehicle communication”, International conference on connected vehicles, (ICCVE), (2015).
[35] Bohml nder, Dennis, et al. Advantages in Crash Severity Prediction using Vehicle to Vehicle Communication." Dependable Systems and Networks Workshops (DSN-W), 2015 IEEE International Conference on. IEEE, 2015.
[36] Warabino, Takayuki, et al. "Adaptive media switching for future vehicle-to-vehicle communication." Personal, Indoor and Mobile Radio Communications, 2005. PIMRC 2005. IEEE 16th International Symposium on. Vol. 2. IEEE, 2005.
[37] Fodor, Gábor, et al. "Device-to-device communications for national security and public safety." Access, IEEE 2 (2014): 1510-1520



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY