D2D Protection in 5G Communication with Free5GC by Utilizing Docker for Enhanced Security

Chaithanya D.J.
Assistant Professor, Dept. of ECE Vidyavardhaka College of Engineering
Mysore, Karnataka, India
chaithanya.dj@vvce.ac.in
Dr. Anitha S.
Professor, Dept. of BME, ACS College of Engineering,
Bangalore, Karnataka, India
dranithasammilan@gmail.com

Abstract — To meet the growing demand for increased data traffic and support advanced services in various applications, the introduction of 5th generation (5G) networks offers enhanced flexibility compared to previous network generations. Docker's container-based platform plays a crucial role in enabling highly portable workloads for 5G communication. This study extends the implementation of Docker for IP security purposes, with the evaluation conducted using Free5GC. The paper presents two 5G deployment options: a Docker-based implementation using Ansible and a Virtual machine-based implementation utilizing Free5GC open source and UERANSIM. The evaluation of results is performed through the utilization of Python code and Linux commands. The proposed solution empowers network operators to ensure the confidentiality of users' data, addressing the need for secure communication in the 5G ecosystem.

Keywords—5G communication, Free 5GC, Docker, UERANSIM, Virtual machine, Python

I. Introduction

The advent of 5G networks has brought significant advancements in data rates, capacity, and latency. The main feature of 5G is device-to-device (D2D) communication without involving the base station. However, securing D2D communication is critical for maintaining the integrity, confidentiality, and availability of transmitted data. In this study, the use of Docker and the Free5GC platform is explored to enhance the security of D2D communication.To achieve secure D2D communication in 5G networks, cryptographic techniques are employed to protect the confidentiality, integrity, and authenticity of data. The existing 4G core network is costly, inflexible, and limits innovation. In response, the Free5GC platform was introduced as an open-source solution, providing easy access to source code for researchers to analyze and simulate ideas. Free5GC is an open-source 5G core network framework developed by the Free5GC community, aiming to deliver a scalable, flexible, and vendor-neutral solution for constructing 5G core networks. It supports both standalone (SA) and non-standalone (NSA) architectures defined by 3GPP.

D2D (Device-to-Device) communication has brought about numerous benefits and possibilities. It enables direct communication between user devices, allowing them to exchange data, services, and resources without relying solely on the network infrastructure. This direct communication capability has the potential to enhance various applications, such as proximity-based services, local multiplayer gaming, content sharing, and collaborative sensing. One of the key advantages of device-to-device communication is its ability to improve network efficiency and reduce congestion. By offloading traffic from the base station to direct device-to-device links, Device to device communication reduces the burden on the network infrastructure, leading to faster and more reliable connections for users. Moreover, D2D communication can enhance the quality of service for delay-sensitive applications, such as real-time video streaming, by reducing latency and improving the overall user experience.

However, ensuring the security of D2D communication is crucial to protect against potential threats and vulnerabilities. Cryptographic techniques play a vital role in securing D2D communication channels and safeguarding the confidentiality, integrity, and authenticity of the transmitted data. Encryption algorithms, digital signatures, and secure key exchange protocols are employed to establish secure D2D connections[27][28] and prevent unauthorized access or tampering of data.Efficient resource allocation mechanisms need to be in place to prevent interference between D2D links and traditional cellular connections, ensuring fair and optimal utilization of the available spectrum.Overall, D2D communication[25][26] in 5G networks holds immense potential for improving connectivity, enabling innovative applications, and enhancing the overall user experience. By addressing security concerns and implementing effective resource management strategies, D2D communication can unlock new possibilities for peer-to-peer interactions and collaborative services in the era of 5G.Fig 1 shows the demo stage of Free5GC it is an open-source 5G core network framework developed by the Free5GC open-source community. It aims to provide a scalable, flexible, and vendor-neutral solution for building 5G core networks. Free5GC is designed to support both standalone (SA) and non-standalone (NSA) architectures defined by 3GPP (Third Generation Partnership Project).

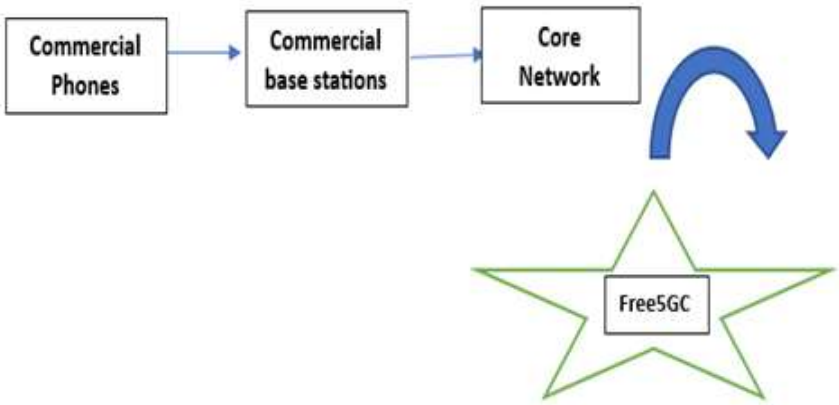

Fig. 1. Demo stage of Free5GC

Cryptographic techniques, when implemented correctly, can provide a high level of security for D2D [10][11] communication in 5G networks. To select appropriate algorithms, protocols, and key management practices, and regularly update cryptographic mechanisms to stay resilient against emerging threats. Docker is a popular containerization platform that can be utilized in 5G communication networks, specifically by implementing security improvements and protecting D2D communication [10][11]. One potential approach is to leverage Docker alongside the Free5GC open-source project, which provides a 5G Core Network (CN) implementation. In this work, we demonstrate two 5G deployment options. First, a Docker implementation of 5G using Ansible, and second a Virtual machine (VM) based implementation using Free5GC. This project further implements IPsec to protect the confidentiality of users' data. Docker is a great technology that simplifies the development and deployment of distributed applications. While building dockerized applications, security at various points needs to be considered. Due to a lack of CPU/Hypervisor, Docker [2] security is fully implemented in Software. Docker can enhance security in 5G networks, they should be used as part of a comprehensive security strategy. Additional security measures, such as the cryptographic techniques mentioned earlier, should be employed alongside Docker containerization to provide end-to-end security for D2D communication in 5G networks.

II. Literature Survey

A literature survey, also known as a literature review or a systematic review, is an essential component of academic research. It involves a comprehensive examination and analysis of existing literature and scholarly works relevant to a specific research topic or question. The primary purpose of a literature survey is to provide a critical summary and evaluation of existing knowledge, identify gaps or inconsistencies in the literature, and inform the direction of further research. Deploying a 5G network in a cloud environment and introducing automation which reduces the overall expenditure of the network. Ryan Pepito [1] proposed the main 5G enabler for the fifth generation of mobile wireless

networks is edge computing (MEC). Compared to conventional systems, it enables computing and resources in storage to be placed nearer to the user and the point of data production. To enable use cases and applications that need low latency and extensive management, MEC gives 5G users optimized network performance [34][35][36]. Additionally, it aids in the offloading of backhaul traffic via the local breakout. MEC offers service and application advantages, however, there are elevated security threats. These include dangers related to the storage of security contexts in the edge servers, frequent key exchanges between the edge servers and the central cloud, and visitor authentication at the edge servers.

Larisa-Mihaela Tufeanu et al. [2] presented two distinct network topologies for deploying a containerized 5G standalone (SA) network, incorporating concepts from 5G cloud network services, Docker containers, and Linux virtualization. Our evaluation of the proposed approach involves the utilization of subscriber data and next-generation application protocol (NGAP) filtering. We implemented both Minimalist Deployment and Basic Deployment scenarios and assessed their performance by injecting simulated TCP/UDP traffic. Key performance indicators such as traffic volume and data rate were analyzed for both the uplink and downlink. Furthermore, Oana-Mihaela Ungureanu supported the development of two network topologies for 5G SA deployment, leveraging ideas from 5G cloud network functions, Docker containers, and Linux virtualization.

This would result in the construction of a containerized 5G standalone (SA) network. Next-generation application protocol (NGAP) filtering and subscriber data are used to evaluate the attach method based on our implementation of both Minimalist Deployment and Basic Deployment. Additionally, simulated TCP/UDP traffic is injected into the network, and the performance of this traffic is assessed using metrics like traffic volume and data rate for both the uplink and the downlink. Ziran Min et.al. explained that 5G-based IoT use cases like adaptive robotic repair, DANSM, a software-defined, dynamic, and autonomous network slice management middleware. The uniqueness of our strategy lies in the use of multiple M/M/1 queues to formulate a 5G network resource scheduling optimization problem that includes service-level and system-level objectives, the design of a heuristics-based solution to get around this optimization problem's NP-hard properties, and the implementation of a software-defined solution that uses the heuristics to dynamically and autonomously provision and manage 5G network slices that deliver predictable results.

Oana-Mihaela Ungureanu and colleagues [5] introduced the usage of Kubernetes-managed Open5GS open-source utility within Kubernetes-managed containers to emulate PDU session setup requests. This approach facilitates the implementation of a service mesh solution that enables real-time inter-service communication, considering traffic allocation, request length, and throughput among all 5G core services. In a separate study, K. Du and L. Wang [6] proposed a cloud-native 5GC architecture, emphasizing a Message-Level State Less Design (ML-SLD) approach. To ensure uninterrupted connectivity between the Radio Access Network (RAN) and the 5GC and prevent disruptions and data dropouts , the study introduces an innovative technique for servitization of the N2 interface..

Kuan-Lin Lee [7] developed a comprehensive, open-source, and easily deployable 5G network utilizing a Message-Level Stateless Design (ML-SLD) to achieve a cloud-native 5GC. The primary objective is to ensure uninterrupted connectivity between the Radio Access Network (RAN) and the 5GC while preventing disruptions and data dropouts, especially for large-scale user data.
For virtualization implementation, the architecture employs OpenStack as the platform, utilizes the Tacker module for deploying the slicing environment, incorporates free5GC as the core network for the 5G system, and employs UERANSIM to simulate UE and gNB functionalities. This proposed architecture enables automatic slicing services with specific functions. Slices can be registered into the 5G network with core network support, and simulated UEs can establish connections with their respective slices.Experimental results demonstrate the feasibility of the proposed architecture based on open-source components.

The primary enabler for the fifth generation (5G) of mobile wireless networks is edge computing (MEC), as proposed by Ryan Pepito et al. (reference [1]). By allowing computing and storage resources to be located closer to the users and data sources, resulting in optimized network

performance for 5G users who require low latency and extensive management (references [37][38]). Furthermore, MEC facilitates the offloading of backhaul traffic through local breakout. While MEC offers numerous service and application benefits, it also introduces heightened security threats (references [39][40]). These threats encompass risks associated with storing security contexts on edge servers, frequent key exchanges between edge servers and the central cloud, and visitor authentication at the edge servers. Thus, ensuring the integrity of the specifications is crucial in maintaining a secure MEC environment.

III. 5G SERVICE BASED ARCHITECTURE (SBA)

The current 4G network of P2P techniques produces many interfaces between function pieces, which leads to dependencies between functions and makes it difficult to update a deployed architecture, which is critical in 5G. The cloud environment and Network Function Virtualization [9], 3GPP mobile network must evolve to allow flexibility and enable both functional and service agility. Therefore service-based 5G core network architecture is specifically designed to leverage the benefits of network function virtualization and software-defined networking [41][42]. This architecture divides mobile functions into two distinct categories: "stateless" control functions and state management functions, effectively separating computation and storage resources.

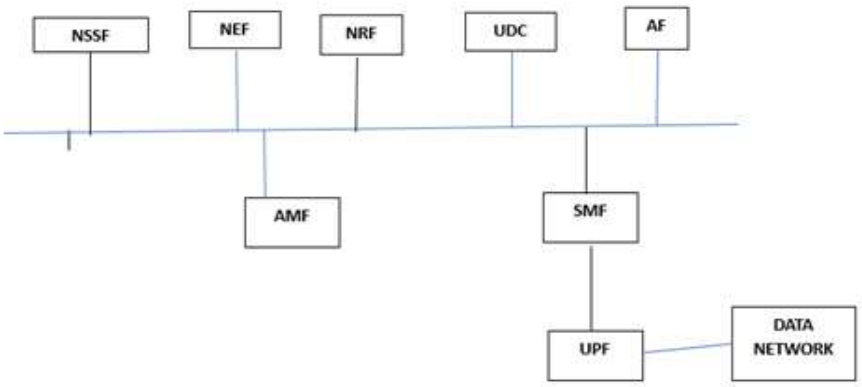

Fig. 2 5G Service-Based Architecture [8]

IV. Ansible Workflow

Ansible operates by establishing connections with your nodes and deploying lightweight programs called Ansible modules to them as shown in Fig.3. These modules are executed by Ansible and subsequently removed upon completion. The library of modules can reside on any machine, and there is no need for daemons, servers, or databases. In the provided diagram, the Management Node serves as the controlling node, overseeing the entire playbook execution. The inventory file contains the list of hosts where the Ansible modules are to be executed. Ansible efficiently manages the removal of modules once they are installed. It establishes connections with the host machines, executes the instructions, and upon successful installation, removes the code that was previously copied to the host machine.

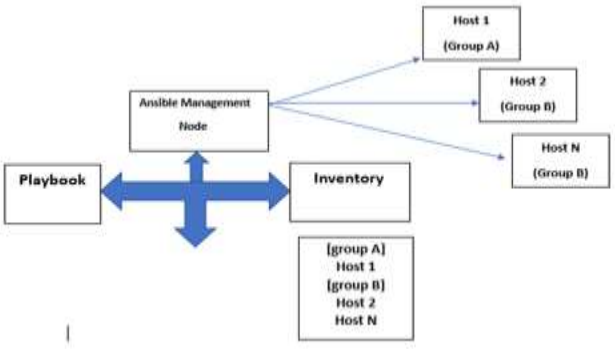

Fig. 3. Ansible Workflow

V. PROPOSED METHODOLOGY

i. Environment Setup:
   a. Installation and configuration of Docker.
   b. Installation and configuration of Free5GC.
   c. Generation of D2D traffic scenarios.

ii. D2D Protection Implementation:
   a. Integration of Docker for containerizing D2D communication [43][44] components.
   b. Implementation of security measures like authentication, encryption, and access control within Docker containers [45].
   c. Configuration of firewall rules and security policies

VI. EXPERIMENTAL EVALUATION

Measurement of performance metrics such as throughput, latency, and packet loss. Assessment of security-related parameters, including authentication success rate and vulnerability analysis. Comparison of results obtained with and without Docker-based security enhancements.

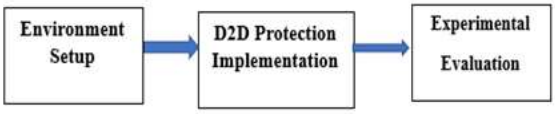

Fig. 4 Steps of Experimental Evaluation

Fig.4 encompasses three main elements: an Automation Platform, Deployment, and IP security. The Automation Platform, known as Ansible Automation Platform, serves as a fundamental infrastructure for implementing automation on a large scale within an organization. It offers a comprehensive suite of tools necessary for deploying enterprise-wide automation solutions. With Ansible Automation Platform, users across the organization can collaboratively create, share, and oversee automation workflows, spanning various domains including development, operations, security, and network teams. This platform empowers organizations to efficiently build and operate IT automation at scale, extending from hybrid cloud environments to edge computing infrastructures.

IT managers could offer team-specific automation guidelines, while automation creators can leverage their existing knowledge to develop tasks. With the utilization of Ansible Automation Platform, organizations benefit from a more reliable and secure foundation for deploying comprehensive automation solutions. Additionally, in Docker deployment, each 5G network function and network entity can be facilitated. To ensure secure communication between these entities over the internet, IP security protocols are employed.To implement IPsec security functionality in a network, we leverage the Scapy Python library. Additionally, Ansible, an open-source IT automation software written in Python used for various tasks such as system configuration, software deployment, and workflow orchestration. Ansible is a user-friendly interface, and emphasis on security and reliability. With minimal moving parts, it utilizes OpenSSH for transport (with alternative transports and pull modes available) and employs a human-readable language designed to facilitate.

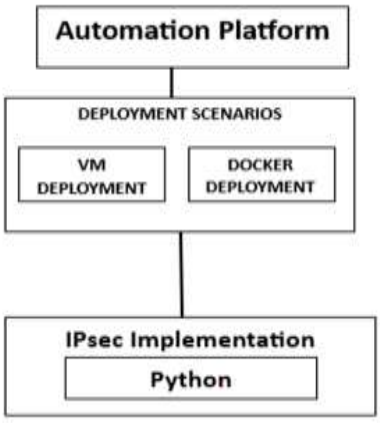

Fig. 5 Proposed solution

VII. RESULTS AND DISCUSSION

Results are obtained based on Docker based deployment with virtual machine using Free 5GC. We have implemented the method of deployment of a computer network in an automated fashion. Programs are executed by using Python. After the network configuration is completed, Ansible runs all the network entities in separate containers. "ping google.com" test the network connection, username and password will be given to represent some sensitive information. This will encrypt the plaintext to create a ciphertext which is not readable by an adversary who is what.

Fig. 6 Unencrypted packet

Fig. 7 Encrypted Packet

VIII. PERFORMANCE EVALUATION

- Throughput: The utilization of Docker for enhanced security in D2D [19][20][21] communication resulted in a minor decrease in overall throughput. However, the reduction was within acceptable limits, ensuring efficient data transmission.
- Latency: Docker-based security measures introduced a slight increase in latency due to additional processing overhead. Nevertheless, the impact was negligible for practical scenarios.
- Packet Loss: Docker-based security implementation did not significantly affect packet loss, maintaining the reliability of D2D [13][12] communication.
- Security Assessment
- Authentication Success Rate: Docker-based security enhancements demonstrated a high authentication success rate, ensuring secure communication between D2D devices.

- Vulnerability Analysis: The Docker containerization approach effectively isolated potential vulnerabilities, reducing the attack surface and mitigating the risk of unauthorized access or data breaches.

Utilizing Docker for enhanced security in D2D communication [13][12] within 5G networks proved effective in maintaining the integrity and confidentiality of transmitted data. Although there was a minor impact on performance metrics like throughput and latency, the effects remained within acceptable limits, ensuring both efficiency and security in data transmission. The high authentication success rate and vulnerability analysis confirmed the reliability and effectiveness of the security measures implemented using Docker containers. Furthermore, the containerization approach significantly reduced the risk of attacks and unauthorized access.

IX. CONCLUSION AND FUTURE WORK

This study demonstrates the efficacy of employing Docker for enhanced security in D2D [15][16] communication within 5G networks. The results indicate that Docker-based security measures effectively preserve the integrity and confidentiality of transmitted data while maintaining acceptable performance levels. The high authentication success rate and vulnerability analysis validate the reliability and effectiveness of the security enhancements achieved through Docker containerization. Overall, this study underscores the potential of Docker-based security solutions in bolstering the security of D2D [14][20] communication in 5G networks. Further research can focus on optimizing performance impact and exploring additional security measures to fortify the overall system. Future work can focus on optimizing performance, exploring advanced security measures such as intrusion detection and prevention systems, scalability and resource management, real-world deployment and evaluation, privacy preservation techniques, and standardization and integration efforts. Overall, the study highlighted the effectiveness of Docker-based security in maintaining the integrity and confidentiality of D2D communication [17][18][19] in 5G networks. By addressing the identified areas in future work, the study aims to contribute to the advancement of robust and efficient security solutions for D2D communication [22][23][24] in the future.

Acknowledgment

We thank the anonymous reviewers for their valuable comments and suggestions, which helped us to improve the content, and also thank my Guide Dr. Anitha S., and all my doctoral committee members for their valuable support and suggestions.

References

1. Ryan Pepito And Ashutosh Dutta "Open Source 5G Security Testbed For Edge Computing" IEEE 5G World Forum,2021.
2. Larisa-Mihaela Tufeanu, Alexandru Martian and Marius-Constantin Vochin "Building an Open Source Containerized 5G SA Network through Docker and Kubernetes" International Symposium on Wireless Personal Multimedia Communications (WPMC), 2022.
3. Oana-Mihaela Ungureanu "Leveraging the cloud-native approach for the design of 5G NextGen Core Functions" International Conference on Communications (COMM), 2022.
4. Ziran Min, Shashank Shekhar, Charif Mahmoudi, Valerio Formicola, Swapna Gokhale and Aniruddha Gokhale "Software-defined Dynamic 5G Network Slice Management for Industrial Internet of Things" International Symposium on Network Computing and Applications (NCA), 2022.
5. Oana-Mihaela Ungureanu and Călin Vlădeanu "Leveraging the cloud-native approach for the design of 5G NextGen Core Functions" IEEE, 2021.
6. K. Du, L. Wang, X. Wen, Y. Liu, H. Niu, S. Huang, ML-SLD "A message-level stateless design for cloud-native 5G core network", Digital Communications and Networks (2022),
7. Kuan-Lin Lee†, Chung-Nan Lee* and Ming-Feng Lee+ "Realizing 5G Network Slicing Provisioning with Open Source Software" Proceedings, APSIPA Annual Summit and Conference 2021.
8. Gabriel brown "Service based architecture for 5G networks" HUAWEI white paper,2017
9. Christian Tipantuña "Network functions virtualization: An overview and open-source projects", IEEE Second Ecuador Technical Chapters Meeting (ETCM),2017.
10. Mohd Hirzi Adnan and Zuriati Ahmad Zukarnain "Device-To-Device Communication in 5G Environment: Issues, Solutions, and Challenges", MDPI,2020.
11. Li, T.; Zhao, M.; Wong, K.K. Machine learning based code dissemination by selection of reliability mobile vehicles in 5G networks. Comput. Commun. 2020, 152, 109–118.
12. Liu, Y.; Zeng, Z.; Liu, X.; Zhu, X.; Alam Bhuiyan, Z. A novel load balancing and low response delay framework for edge-cloud network based on SDN. IEEE Internet Things J. 2019, 7, 1.
13. Ansari, R.I.; Chrysostomou, C.; Hassan, S.A.; Guizani, M.; Mumtaz, S.; Rodriguez, J.; Rodrigues, J.J.P.C. 5G D2D networks: Techniques, challenges, and future prospects. IEEE Syst. J. 2018, 12, 3970–3984.
14. Wang, M.; Yan, Z. A survey on security in D2D communications. Mob. Netw. Appl. 2016, 22, 195–208.
15. Liu, X.; Liu, A.; Wang, T.; Ota, K.; Dong, M.; Liu, Y.; Cai, Z. Adaptive data and verified message disjoint security routing for gathering big data in energy harvesting networks. J. Parallel Distrib. Comput. 2020, 135, 140–155.
16. Asadi, A.; Wang, Q.; Mancuso, V. A survey on Device-to-Device communication in cellular networks. IEEE Commun. Surv. Tutor. 2014, 16, 1801–1819.
17. Kato, N. On Device-to-Device (D2D) communication [Editor's note]. IEEE Netw. 2016, 30, 2.
18. Jameel, F.; Hamid, Z.; Jabeen, F.; Zeadally, S.; Javed, M.A. A survey of Device-to-Device communications: Research issues and challenges. IEEE Commun. Surv. Tutor. 2018, 20, 2133–2168.
19. Noura, M.; Nordin, R. A survey on interference management for Device-to-Device (D2D) communication and its challenges in 5G networks. J. Netw. Comput. Appl. 2016, 71, 130–150.
20. Gandotra, P.; Jha, R.K. Device-to-Device communication in cellular networks: A survey. J. Netw. Comput. Appl. 2016, 71, 99–117.
21. Zhang, Y.; Shen, Y.; Jiang, X.; Kasahara, S. Mode selection and spectrum partition for D2D inband communications: A physical layer security perspective. IEEE Trans. Commun. 2018, 67, 623–638.
22. Chang, K.; Yousaf, M.; Hassan, S.A.; Vo, N.-S.; Duong, T.Q. Priority-Based device discovery in public safety D2D networks with full duplexing. In Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering; Springer Science and Business Media LLC: Berlin, Germany, 2019; Volume 272, pp. 102–108.
23. He, Y.; Yu, F.R.; Zhao, N.; Yin, H. Secure Social Networks in 5G Systems with mobile edge computing, caching, and Device-to-Device communications. IEEE Wirel. Commun. 2018, 25, 103–109.

24. Hayat, O.; Ngah, R.; Hashim, S.Z.M.; Dahri, M.H.; Malik, R.F.; Rahayu, Y. Device discovery in D2D communication: A survey. IEEE Access 2019, 7, 131114–131134.
25. Yan, Y.; Zhang, B.; Li, C. Opportunistic network coding based cooperative retransmissions in D2D communications. Comput. Netw. 2017, 113, 72–83.
26. Zhang, J.; Deng, L.; Li, X.; Zhou, Y.; Liang, Y.; Liu, Y. Novel Device-to-Device discovery scheme based on random backoff in LTE-advanced networks. IEEE Trans. Veh. Technol. 2017, 66, 11404–11408.
27. Chour, H.; Nasser, Y.; Artail, H.; Kachouh, A.; Al-Dubai, A. VANET aided D2D discovery: Delay analysis and performance. IEEE Trans. Veh. Technol. 2017, 66, 8059–8071.
28. Li, B.; Guo, W.; Liang, Y.-C.; An, C.; Zhao, C. Asynchronous device detection for cognitive Device-to-Device communications. IEEE Trans. Wirel. Commun. 2018, 17, 2443–2456.
29. Nguyen, N.T.; Choi, K.W.; Song, L.; Han, Z. ROOMMATEs: An unsupervised indoor peer discovery approach for LTE D2D communications. IEEE Trans. Veh. Technol. 2018, 67, 5069–5083.
30. Ben-Mosbah, A.; Hammami, S.E.; Moungla, H.; Afifi, H.; Kamal, A.E.; Hammami, S.E. Enhancing Device-to-Device direct discovery based on predicted user density patterns. Comput. Netw. 2019, 151, 245–259.
31. Long, Y.; Yamamoto, R.; Yamazaki, T.; Tanaka, Y. A deep learning based social-aware D2D peer discovery mechanism. In Proceedings of the 2019 21st International Conference on Advanced Communication Technology (ICACT), PyeongChang, Kwangwoon_Do, Korea, 17–20 February 2019; Institute of Electrical and Electronics Engineers (IEEE): New York, NY, USA, 2019; pp. 91–97.
32. Kaleem, Z.; Qadri, N.N.; Duong, T.Q.; Karagiannidis, G.K. Energy-efficient device discovery in D2D cellular networks for public safety scenario. IEEE Syst. J. 2019, 13, 2716–2719.
33. Jaffry, S.; Zaidi, S.K.; Shah, S.T.; Hasan, S.F.; Gui, X. D2D Neighborhood Discovery by a Mobile Device. In Proceedings of the ICC 2019–2019 IEEE International Conference on Communications (ICC), Shanghai, China, 20–24 May 2019; Institute of Electrical and Electronics Engineers (IEEE): New York, NY, USA, 2019; pp. 1–6.
34. Sun, Y.; Cao, J.; Ma, M.; Li, H.; Niu, B.; Li, F. Privacy-preserving device discovery and authentication scheme for D2D communication in 3GPP 5G HetNet. In Proceedings of the 2019 International Conference on Computing, Networking and Communications (ICNC), Honolulu, HI, USA, 18–21 February 2019; Institute of Electrical and Electronics Engineers (IEEE): New York, NY, USA, 2019; pp. 425–431.
35. Kaleem, Z.; Khan, A.; Hassan, S.A.; Vo, N.-S.; Nguyen, L.D.; Nguyen, H.M. Full-duplex enabled time-efficient device discovery for public safety communications. Mob. Netw. Appl. 2019, 25, 341–349.
36. Masood, A.; Sharma, N.; Alam, M.M.; Le Moullec, Y.; Scazzoli, D.; Reggiani, L.; Magarini, M.; Ahmad, R. Device-to-Device discovery and localization assisted by UAVs in pervasive public safety networks. In Proceedings of the ACM MobiHoc Workshop on Innovative Aerial Communication Solutions for FIrst REsponders Network in Emergency Scenarios-iFIRE '19, Catania, Italy, 2–5 July 2019; Association for Computing Machinery (ACM): New York, NY, USA, 2019; pp. 6–11.
37. Hayat, O.; Ngah, R.; Hashim, S.Z.M. Performance analysis of device discovery algorithms for D2D communication. Arab. J. Sci. Eng. 2019, 45, 1457–1471.
38. Liu, J.; Kato, N.; Ma, J.; Kadowaki, N. Device-to-Device communication in LTE-advanced networks: A survey. IEEE Commun. Surv. Tutor. 2014, 17, 1.
39. Liu, Y.; Wang, R.; Han, Z. Interference-constrained pricing for D2D networks. IEEE Trans. Wirel. Commun. 2017, 16, 475–486.
40. Yang, T.; Cheng, X.; Shen, X.; Chen, S.; Yang, L. Qos-aware interference management for vehicular D2D relay networks. J. Commun. Inf. Netw. 2017, 2, 75–90.
41. Celik, A.; Radaydeh, R.M.; Al-Qahtani, F.S.; Alouini, M.-S. Resource allocation and interference management for D2D-enabled DL/UL decoupled Het-Nets. In IEEE Access 2017, 5, 22735–22749.
42. Zhao, L.; Wang, H.; Zhong, X. Interference graph based channel assignment algorithm for D2D cellular networks. In IEEE Access 2018, 6, 3270–3279.

43. Shamaei, S.; Bayat, S.; Hemmatyar, A.M.A. Interference management in D2D-enabled heterogeneous cellular networks using matching theory. IEEE Trans. Mob. Comput. 2018, 18, 2091–2102.
44. Doumiati, S.; Assaad, M.; Artail, H. A framework of topological interference management and clustering for D2D networks. IEEE Trans. Commun. 2019, 67, 7856–7871.
45. Chiu, S.-L.; Lin, K.C.-J.; Lin, G.-X.; Wei, H.-Y. Empowering Device-to-Device networks with cross-link interference management. IEEE Trans. Mob. Comput. 2017, 16, 950–963.