MAC Independent IP Allocation for Seamless Connectivity in Mobile Networks by Dynamic Host Configuration Protocol

Sravan kumar Gurram[1],MD Fakeer baba[2],Narsaiah Battu[3] and Namilakonda Sumanjali[4]
[1]*Asst.professor,Dept.of CSE, JNTUH University College of Engineering,Jagtial,Telangana,India.*
[2]*Asst.professor,Dept.of CSA, Govt Degree College,Sircilla,Telangana,India.*
[3]*Asst.professor,Dept.of CSA, Dr.B.R.Ambetkar Open University,Hyderabad,Telangana,India.*
[4]*Asst.professor,Dept.of Data Science, CMREC,Hyderabad,Telangana,India.*

***Abstract*— Mobile network also called as cellular network. It is an instance of the wireless network. Mobile network is collection of base stations/towers, which are setup strategically to cover a specific geographical area. Mobile nodes in these type network moves unpredictably among base stations. In order to start the communication every device needs IP configuration, which will be allocated dynamically by DHCP (dynamic host configuration protocol) by default. Once 50% of the lease time is completed it will be renewed based on the request from DHCP client and availability of IP addresses in the IP pool. Every time a mobile device is connected to the access point in the mobile network it will allocated an IP configuration information without relating to its MAC (media access control) address. IP configuration include IP address, subnet mark, default gateway and DNS (domain name system) server.**

Keywords— ***Dynamic IP Allocation, DHCP, Mobile Networks, IP Configuration, IP Pool.***

I. INTRODUCTION

A mobile network is an instance of the wireless network, that allows wireless communication among mobile devices such as smartphones, tablets, IoT devices, and Unnamed Area Vehicles (UAV). This communication is possible by connecting mobile devices to base stations or towers in the network. These towers will be set strategically to cover the specific geographical area, which provide communication between mobile devices and the wider telecommunications system. To facilitate communication between devices, mobile networks employ various technologies such as GSM (Global System for Mobile Communications), CDMA (Code Division Multiple Access), LTE (Long Term Evolution), and 5G[1]. Cellular network architecture is shown in **Error! Reference source not found.**[2].

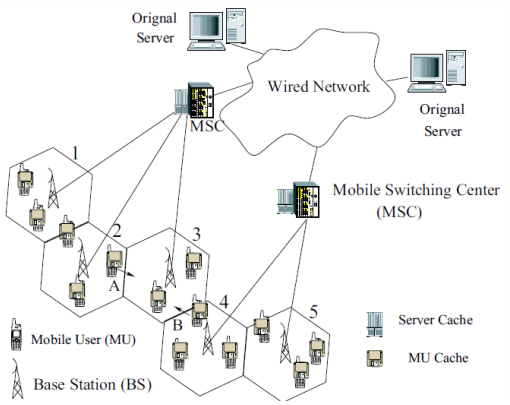

Figure 1: Cellular Network Architecture

Mobile devices in the mobile network moves frequently among various access points. When a mobile device connects to an access point it needs IP configuration information to start communication in the network. The IP configuration plays a vital in effective communication in the mobile network. The responsibility of assigning IP configuration to the mobile device lies with the Dynamic Host Configuration Protocol (DHCP)[3].This process includes mobile device requests for IP configuration from DHCP server and server acknowledge to assign IP configuration, shown in **Error! Reference source not found.**.

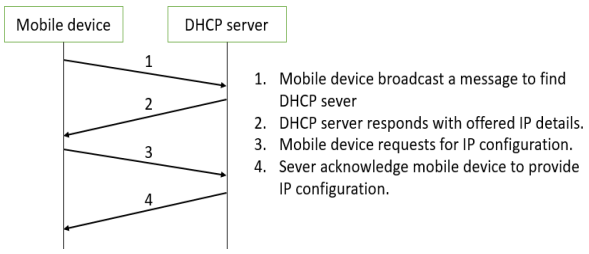

Figure 2: Mobile device request process for IP Configuration

Proper IP allocation by DHCP insures that every mobile device gets a unique IP address for effective

communication. IP configuration allocation includes the allocation of subnet masks, default gateways, and DNS server to facilitate data exchange besides IP address[4] .

Moreover, the IPv6 can be used in future to tackle the need for increased demand for IP address. IPv6 has provide large IP pool compared to IPv4. This transition to IPv6 will facilitate the rising number of mobile devices in mobile networks, guaranteeing scalability and securing the allocation of IP addresses for the future. By implementing IPv6, mobile networks can efficiently and flexibly assign a vast array of IP addresses to accommodate the expanding number of devices. Additionally, the adoption of IPv6 will foster the expansion of networks by enabling the utilization of cutting-edge technologies like IoT (Internet of Things) and 5G connectivity.

II. LITERATURE SURVEY

Number of mobile devices are rapidly increasing now a days and relying on IP configuration in mobile networks[5]. Due to the use of this rapidly rising mobile devices like IoT devices and unnamed area vehicles caused a shortage of IP addresses. Consequently, allocating IP addresses to mobile devices is challenging task. One solution is to use IPv6, which offers a large pool of IP addresses. By doing so, day to day increasing devices in the mobile network can allocated addresses dynamically and each device gets unique IP address. This transition will provide a large IP pool in number of addresses, so that all future devices can be addressed effectively[6]. One possible improvement is that DHCP server allocates IP address dynamically to the mobile device for a specific period of time known as lease time[7]. So that every node gets IP address. Furthermore, by using network address translation (NAT) IP addresses can be preserved by reserving same IP address for multiple devices. NAT also secure internal IP addresses from outside IP addresses. This can mitigate the need for IPv4 addresses and extending their availability of IP addresses among mobile devices[8]. Furthermore, network function virtualization (NFV) is capable of enhancing IP allocation through dynamic allocation mechanism and management of virtualized IP resources. NFV also improve flexibility and scalability in IP address allocation, enabling the provision of IP addresses for mobile and IoT devices as and when required. This results in effective use of IP resources and support the growing demand for devices in mobile networks[9]. Finally, with the use of IPv6 wider range IP addresses available in the pool. The increasing devices in the network can be addressed dynamically without any IP conflict. Moreover, IPv6 facilitate emerging technologies, including 5G and 6G networks, the Internet of Things, UAV etc.

In the end of the literature survey, it is concluded that mobile networks require an effective dynamic IP configuration allocation.

III. DYNAMIC HOST CONFIGURATION PROTOCOL

The use of mobile devices in the mobile networks is increasing day by day. Due to the increasing mobile devices it becomes challenging task to assign IP addresses effectively. DHCP server is the solution which can allocate IP addresses dynamically. This automated process of IP allotment mitigate the burden on network administrators[10]. DHCP is the default protocol used by the most of the routers and networking equipment.

- DHCP manages the provision of all the nodes or devices added or dropped from the network.
- DHCP maintains the unique IP address of the host using a DHCP server.
- It sends a request to the DHCP server whenever a client/node/device, which is configured to work with DHCP, connects to a network. The server acknowledges by providing an IP address to the client/node/device.

The following are DHCP components involved in mobile networks:

1. DHCP server: The DHCP server functions as a networked device that operates the DHCP service, storing IP addresses and associated configuration details. This device is commonly a server or a router, although it can also be any other type of host.
2. DHCP client: The DHCP client is the recipient of configuration details from a DHCP server. This could be any type of device, such as a computer, laptop, IoT endpoint, or any other device that needs to connect to the network. The majority of devices are set up to automatically receive DHCP information.
3. IP Address pool: The IP address pool refers to the set of addresses that DHCP clients can utilize. Generally, IP addresses are distributed

in a sequential manner, starting from the lowest address and progressing to the highest.

4. Subnet: Subnets are segmented portions of IP networks that are utilized to maintain network manageability.

5. Lease: The duration for which a DHCP client retains the IP address information is referred to as the lease period. Upon expiration of the lease, the client is required to renew it.

DHCP also provides other configuration information to the devices, such as subnet masks, default gateways, and DNS (Domain Name System) server addresses, ensuring that the devices can communicate effectively on the network and connect to necessary network resources. This dynamic allocation of IP addresses also helps in preventing IP address conflicts on the network, ensuring smooth communication between devices.

Error! Reference source not found. represents IP configuration allocated to a mobile device by DHCP server.

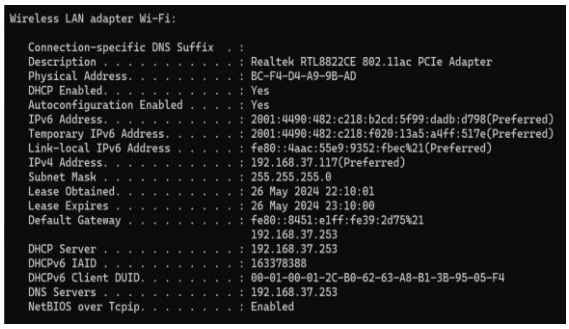

Figure 3: IP Configuration allocation 1

DHCP assigns an IP address to the mobile device for period of time called lease time. Mobile device sends a request to the server for renewal of IP address after 50% of the lease time is completed. Therefore, communication will be done smoothly[11]. DHCP maintains IP pool with contains all available addresses, from which it assigns IP address to the connected device. The server maintains IP pool centrally so that it can be easily controlled or maintained by the administrator. Additionally, DHCP server supports a specific feature to assign a specific IP address to devices based their MAC address (physical address) every time it is connected to the network[12]. This feature is useful when a device needs static IP address. For example a printer in net café is allocated with a static IP address no security issues will be there. But this is not useful as far as security of a device which is frequently moving among different access points in mobile network. Overall, DHCP server greatly reduce the network administrator's burden to maintain IP address pool and assign IP address to mobile devices dynamically[13]. DHCP servers also provide the provision to define lease time of IP address. Once this time period is expired device will be de-allocated with current IP address. So that IP addresses will be allocated to all devices efficiently. Depending upon the network type and expected device count in the network, lease time will be set by the network administrator. This allows for the efficient use of available IP addresses and helps in optimizing network performance[14]. Additionally, DHCP servers also provide other IP configuration information such as default gateway, subnet mask, further simplifying network administration and reducing the possibility of configuration errors[15].

IV. METHODOLOGY AND RESULTS

With the rising number of mobile devices, DHCP may face challenges in assigning IP addresses to all mobile devices using IPv4. Federica Laricchia, a researcher in the Technology and Telecommunications team at Statista, reported that the global count of mobile devices reached nearly 15 billion in 2021, surpassing the previous year's figure of just over 14 billion. Projections indicate that the number of mobile devices will further rise to 18.22 billion by 2025, marking a significant increase of 4.2 billion devices compared to the levels observed in 2020[16]. Shown in the **Error! Reference source not found.**

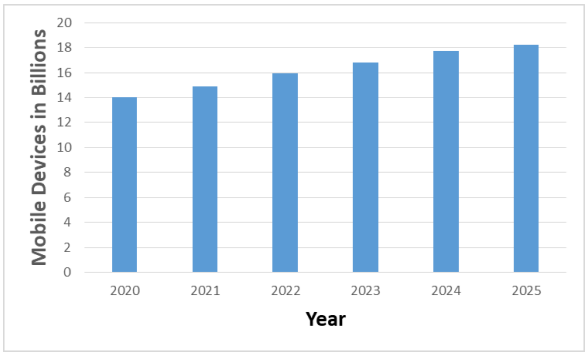

Figure 4: Year wise account of Mobile devices

Since devices in mobile network leave and join the network unpredictably .It is challenging task to DHCP to assign IP to devices. The rise of IoT devices in mobile networks brings about issues such as ineffective access control and inadequate

authentication[17]. Moreover, the movement of end-devices in networks necessitates the use of resource allocation to avoid data loss, underscoring the importance of mobility-aware assignment strategies[18]. Additionally, the transition to distributed network architectures calls for new decision-making mechanisms for optimal base station assignment to mobile devices, improving system throughput while efficiently managing resources[19]. Overcoming these obstacles requires innovative approaches such as agile edge computing systems, proactive resource allocation, and distributed assignment algorithms to ensure smooth IP address assignment in dynamic mobile environments.

Mobile devices within mobile networks have the ability to freely transition between different base stations (access points) in a dynamic manner. The network diagram (**Error! Reference source not found.**) provided depicts a real-time experiment scenario in which mobile devices can move seamlessly among three access points.

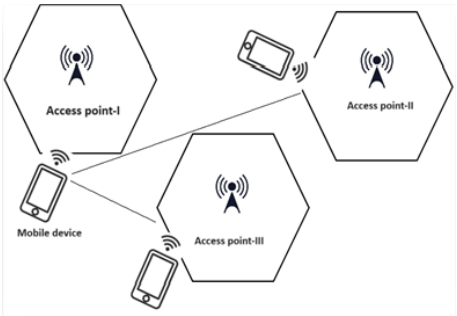

Figure 5: Mobile network with three access points

During my research into the allocation of IP configurations by a DHCP server to a mobile device that moves between various accesses points in a mobile network, I examined three real-time access points.

1. Access point-I: It is a WiFi (wireless fidelity) network access point taken from SR University, Telangana,India. This network is public network to all the employees of that university.
2. Access point-II & III: These are two different private WiFi access points owned by individuals.

A. Access Point-I:

When a mobile device is connected to the access point-I (**Error! Reference source not found.**), which is organizational network (sru.edu.in) . It allocated IP configuration at two different instances as (**Error! Reference source not found.**,**Error! Reference source not found.**)

The mobile device was connected to access point-I on 27th May 2024 in the first allocation. It was assigned the IP address 10.2.9.237 with a lease time of 7 days, from 27th May 2024 to 4th June 2024. In the second allocation, on 5th May 2024, the same mobile device connected to the same access point-I after the IP address had expired. Surprisingly, the device was allocated the same IP address as in the first allocation, even though the lease time had already expired.

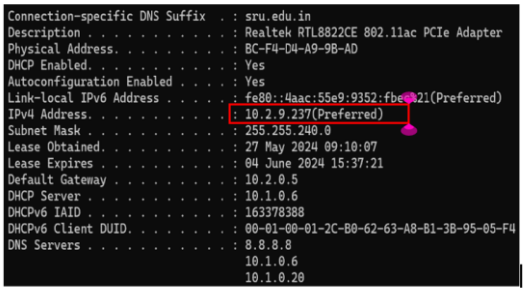

Figure 6: IP configuration allocation 1(Access point-I)

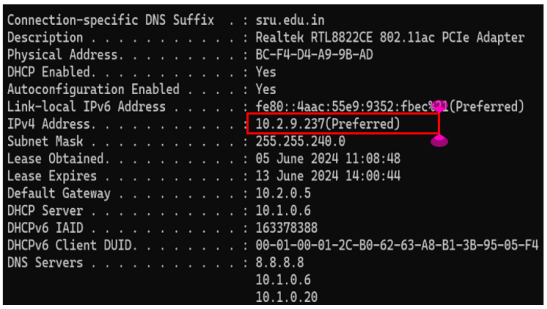

Figure 7: IP configuration allocation 2(Access Point-II)

B. Access Point-II:

Access point-II is private WiFi access point owned by an individual. When the same mobile device is connected to the access point-II, moving from access point-I. DHCP server allocated IP configuration as: (**Error! Reference source not found.**, **Error! Reference source not found.**)

The same mobile device now connected to the access point-II on 26th May 2024. In the first allocation it was assigned the IP address, 172.20.10.9 with a lease time of 1 day (i.e. next day midnight). In the second allocation, on 20th June 2024, the same mobile device connected to the same access point-II after the IP address had expired. Surprisingly, the device was allocated the same IP address as in the first allocation, even though the lease time had already expired.

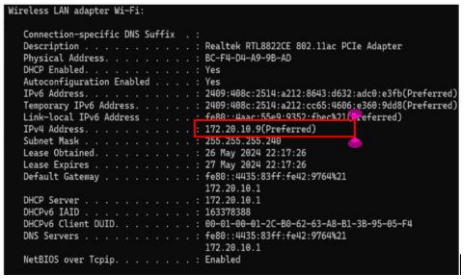

Figure 8:IP Configuration allocation 1 (Access Point-II)

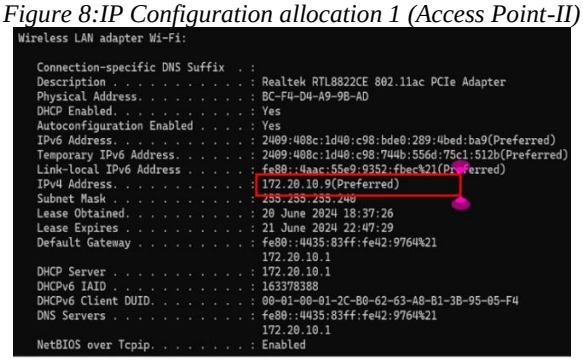

Figure 9: IP Configuration allocation 2 (Access Point-II)

C. Access Point-III:

Access point-III is private WiFi access point owned by an individual. When the same mobile device is connected to the access point-III, moving from access point-I or access point -II. DHCP server allocated IP configuration as (**Error! Reference source not found.**,**Error! Reference source not found.**):

The same mobile device in observation III is connected to the access point-III on 24th June 2024. In the first allocation it was assigned the IP address, 192.168.215.117 with a lease time of 1 hour. In the second allocation, on 24th June 2024, the same mobile device connected to the same access point-III after the IP address had expired. Surprisingly, the device was allocated the same IP address as in the first allocation, even though the lease time had already expired.

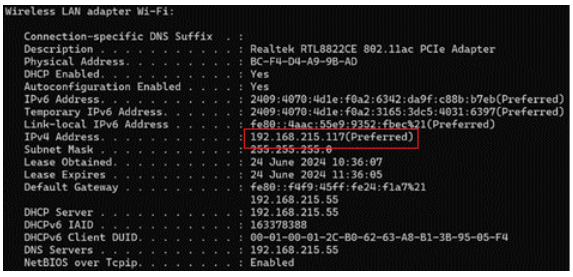

Figure 10: IP Configuration allocation1 (Access Point-III)

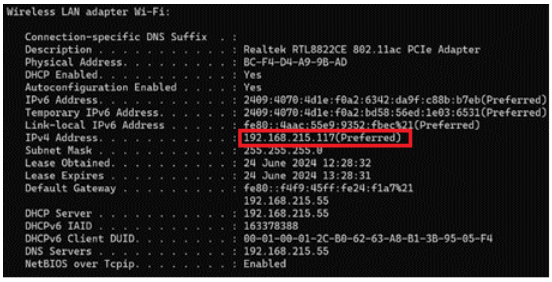

Figure 11: IP Configuration allocation 2(Acceess Point-III)

Observation from the above scenario is shown in the **Error! Reference source not found.**:

TABLE I. IP ALLOCATION BY VARIOUS NETWORKS

Access point type	IP address allocation	Lease time
I: Organizational network	10.2.9.237 (Same IP address allocated in two allocations.	1 week (7 days)
II: personal network	172.20.10.9 (Same IP address allocated in two allocations.	1 day
III: personal network	192.168.215.117 (Same IP address allocated in two allocations.)	1 hour

It has been noted that regardless of how many times a mobile device is connected to any of the three access points, the DHCP server assigns the same IP address to the device even after the lease time has elapsed. The allocation of IP addresses by DHCP is done according to the MAC address of the device. Allocating the same address each time increases the vulnerability of the network to potential attackers, as they can more easily target and compromise the IP address. Such a practice goes against the principles of DHCP, which should assign IP addresses to devices randomly from the pool of available addresses upon connection to a mobile network.

The server allocates IP address to the mobile devices by the following algorithm 1

1. IP[N] ←IP_{addr1} to IP_{addrN} // IP[N] represents collection of addresses .N←0 to 255
2. For all M (0 to 255)

flag[M] ←1

3. $DHCP_{addr}$←IP[0]
4. For all mobile devices connected to a access point

do

a. Client broadcast a DHCP request message
b. DHCP acknowledge with IP address.

c. RIP_{no}=random(1 to 255)
d. If flag[RIP_{no}]=1

assign IP[RIP_{no}] to a mobile device

flag[RIP_{no}] ←0
e. else

goto step c
5. When a device is dis-connected from the access point flag[RIP_{no}] ←1
6. end

Error! Reference source not found. depicts mobile network simulation. Here 5 mobile devices, one access point and one DHCP server is taken. DHCP server is assigned with IP address 172.16.0.1 and subnet mask 255.255.255.0. DHCP dynamically allocates IP addresses to mobile devices to the access point from the address pool 254 IP addresses from 172.16.0.2 to 172.16.0.255. All mobile devices gets IP addresses dynamically when connected to the access point.
Eg: MOBILE DEVICE-III is allocated with IP address 172.16.0.10 by the server.

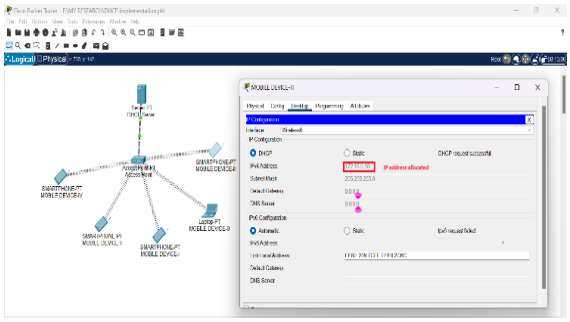

Figure 12: IP allocation to mobile devices by DHCP server.

Mobile devices free to move from once access point to another in mobile networks. Assume that the MOBILE DEVICE-III is moving away from the access point, then it will be disconnected from the access point (**Error! Reference source not found.**).

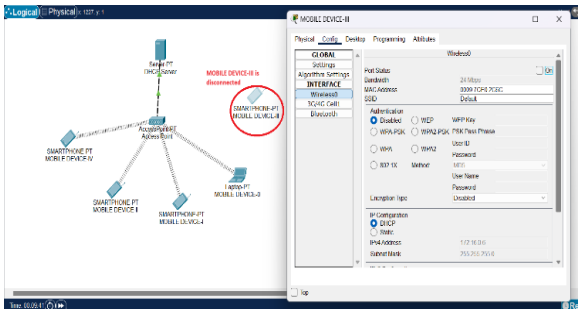

Figure 13: MOBILE DEVICE-III is disconnected from access point.

When the MOBILE DEVICE-III is reconnected to the access point DHCP allocated IP address (172.16.0.3) dynamically to the device (**Error! Reference source not found.**), which is different from the previous IP address. Therefore we can say that the server is not considering physical address of the mobile device while allocating IP address. This way of random IP allocation will prevent attacks on the mobile networks.

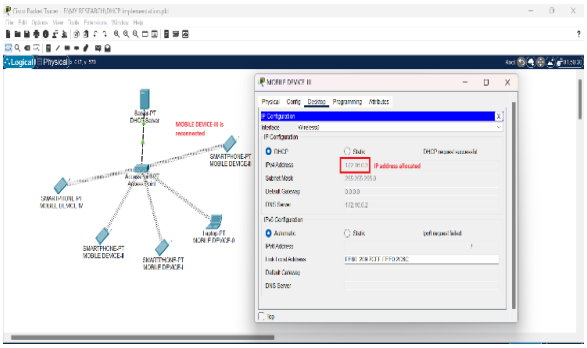

Figure 14: MOBILE DEVICE-III is reconnected with different IP address.

V. CONCLUSION

The mobile network is a type of wireless network where mobile nodes have the freedom to move between access points. Each time a mobile node connects to the network, the DHCP server dynamically assigns an IP address from the available pool of addresses. By allocating IP addresses without relying on the physical address of the device, potential attacks on the network can be prevented. This approach also helps minimize the burden on the network administrator due to the dynamic allocation process. Currently, this system is implemented using IPv4, which allows for a maximum number of mobile devices to be allocated addresses. However, if the number of devices exceeds the available pool of IPv4 addresses, IPv6 can be utilized to allocate addresses to mobile devices.

ACKNOWLEDGMENT

I thank Dr.Vishwanath, asst.prof, SR University, Warangal, India for his support in using different tools and preparation of manuscript and his continuous support through this research work and simulation.

REFERENCES

[1] R. N. Kostoff, P. Heroux, M. Aschner, and A. Tsatsakis, “Adverse health effects of 5G mobile networking technology under real-life conditions,” Toxicol. Lett., vol. 323, pp. 35–40, May 2020, doi: 10.1016/j.toxlet.2020.01.020.

[2] Z. Wang, M. Kumar, S. K. Das, and H. Shen, "Dynamic cache consistency schemes for wireless cellular networks," IEEE Trans. Wirel. Commun., vol. 5, no. 2, pp. 366–376, Feb. 2006, doi: 10.1109/TWC.2006.1611060.

[3] D. A. Pradana and A. S. Budiman, "The DHCP Snooping and DHCP Alert Method in Securing DHCP Server from DHCP Rogue Attack," IJID Int. J. Inform. Dev., vol. 10, no. 1, pp. 38–46, Jun. 2021, doi: 10.14421/ijid.2021.2287.

[4] M. A. Sarvghadi and T.-C. Wan, "Distributed and Efficient Slot Assignment–Alignment Protocol for Resource-Constrained Wireless IoT Devices," IEEE Internet Things J., vol. 10, no. 10, pp. 8754–8772, May 2023, doi: 10.1109/JIOT.2022.3232335.

[5] G. Yang, Y. Liao, Y.-C. Liang, and O. Tirkkonen, "Reconfigurable Intelligent Surface Empowered Underlaying Device-to-Device Communication," in 2021 IEEE Wireless Communications and Networking Conference (WCNC), Nanjing, China: IEEE, Mar. 2021, pp. 1–6. doi: 10.1109/WCNC49053.2021.9417307.

[6] F.Gont, J.Z, and R.Patterson, "Reaction of IPv6 Stateless Address Autoconfiguration (SLAAC) to Flash-Renumbering Events," RFC 8978, vol. 8978, pp. 1–11, Mar. 2021.

[7] M. A. Al-Shareeda, S. Manickam, M. A. Saare, and N. B. Omar, "SADetection: Security Mechanisms to Detect SLAAC Attack in IPv6 Link-Local Network," Informatica, vol. 46, no. 9, Jan. 2023, doi: 10.31449/inf.v46i9.4441.

[8] Y. Meidan, V. Sachidananda, H. Peng, R. Sagron, Y. Elovici, and A. Shabtai, "A novel approach for detecting vulnerable IoT devices connected behind a home NAT," Comput. Secur., vol. 97, p. 101968, Oct. 2020, doi: 10.1016/j.cose.2020.101968.

[9] Nan and Shi Yuan, "In depth analysis on secure socket layer-transport layer security (SSL-TLS) security flaws," Manyang Technol. Univ., 2024, [Online]. Available: https://hdl.handle.net/10356/174981

[10] N. A. Tuan, T. Q. Hung, N. T. Hung, N. T. Dong, and D. V. Quan, "Caching and Containerization of IP Address Allocation Process in 5G Core Networks for Performance Improvements," in 2023 17th International Conference on Ubiquitous Information Management and Communication (IMCOM), Seoul, Korea, Republic of: IEEE, Jan. 2023, pp. 1–8. doi: 10.1109/IMCOM56909.2023.10035655.

[11] N. Hubballi and N. Tripathi, "A closer look into DHCP starvation attack in wireless networks," Comput. Secur., vol. 65, pp. 387–404, Mar. 2017, doi: 10.1016/j.cose.2016.10.002.

[12] L. Jouans, A. C. Viana, N. Achir, and A. Fladenmuller, "Associating the Randomized Bluetooth MAC Addresses of a Device," in 2021 IEEE 18th Annual Consumer Communications & Networking Conference (CCNC), Las Vegas, NV, USA: IEEE, Jan. 2021, pp. 1–6. doi: 10.1109/CCNC49032.2021.9369628.

[13] L. Trombeta and N. M. Torrisi, "DHCP Hierarchical Failover (DHCP-HF) Servers over a VPN Interconnected Campus," Big Data Cogn. Comput., vol. 3, no. 1, p. 18, Mar. 2019, doi: 10.3390/bdcc3010018.

[14] H. M. J. Almohri, L. T. Watson, and D. Evans, "Predictability of IP Address Allocations for Cloud Computing Platforms," IEEE Trans. Inf. Forensics Secur., vol. 15, pp. 500–511, 2020, doi: 10.1109/TIFS.2019.2924555.

[15] D. Bringhenti, R. Sisto, and F. Valenza, "A novel abstraction for security configuration in virtual networks," Comput. Netw., vol. 228, p. 109745, Jun. 2023, doi: 10.1016/j.comnet.2023.109745.

[16] federica-laricchia, "Forecast number of mobile devices worldwide from 2020 to 2025 (in billions)." Mar. 10, 2023. [Online]. Available: https://www.statista.com/statistics/245501/multiple-mobile-device-ownership-worldwide/

[17] D. Wu, X. Huang, X. Xie, X. Nie, L. Bao, and Z. Qin, "LEDGE: Leveraging Edge Computing for Resilient Access Management of Mobile IoT," IEEE Trans. Mob. Comput., vol. 20, no. 3, pp. 1110–1125, Mar. 2021, doi: 10.1109/TMC.2019.2954872.

[18] A. Farhad, D.-H. Kim, B.-H. Kim, A. F. Y. Mohammed, and J.-Y. Pyun, "Mobility-Aware Resource Assignment to IoT Applications in Long-Range Wide Area Networks," IEEE Access, vol. 8, pp. 186111–186124, 2020, doi: 10.1109/ACCESS.2020.3029575.

[19] E. A. Esquivel-Mendiola, H. Galeana-Zapién, D. H. Covarrubias, and E. Aldana-Bobadilla, "Distributed Algorithm for Base Station Assignment in 4G/5G Machine-Type Communication Scenarios with Backhaul

Limited Conditions," Sensors, vol. 20, no. 22,
p. 6553, Nov. 2020, doi: 10.3390/s20226553.