Journal of
Information Systems Engineering
and Business Intelligence

Vol.6, No.1, April 2020
Available online at: http://e-journal.unair.ac.id/index.php/JISEBI

Device-to-Device Communications in Cloud, MANET and Internet of Things Integrated Architecture

Tanweer Alam[*]

Faculty of Computer and Information Systems, Islamic University of Madinah, Saudi Arabia
Prince Naif bin Abdulaziz Road, Madinah
tanweer03@gmail.com

Article history:

Received 14 January 2020
Revised 12 March 2020
Accepted 13 March 2020
Available online 28 April 2020

Keywords:

5G Network
Ad-Hoc Networks
Cloud
Internet of Things
Mobility
Smart Devices

Abstract

Background: The wireless networks make it easier for users to connect with each other in the sense of the Internet of Things (IoT) system. The cloud and MANET convergence offer the services for cloud access within MANET of devices connected.
Objective: The main objective of this research is to establish a cloud-based ad-hoc network architecture for the communication among smart devices under the 5G based Internet of Things architecture.
Methods: The methods are applied to discover the smart devices using probability-based model, hidden Markov model and gradient-based model.
Results: A cloud-MANET architecture of the smart device is constructed with cloud and MANET computation. The framework allows MANET users to access and deliver cloud services through their connected devices, where all simulations, error handling, and resource management are implemented.
Conclusion: The MANET service has been launched as well as linked to the cloud by the mobile device. The author used the amazon cloud storage service. This research produces a conceptual model that is based on the ubiquitous method. It is shown the success in this area and expectations for future scope.

I. INTRODUCTION

This study is a move forward over the cloud, MANET, and internet of things in 5G diverse systems where the author proposes a novel framework for the mobility model using cloud computing to communicate in a 5G network of smart devices on the internet [1]. In the article [2], the authors explained the device to device communication under the cellular networks. The Device-to-Device (D2D) communication within phone networks is represented as communicating directly among two smartphone users without attempting to cross the base station. The proposed study could be used to improve and expand current MANET communication using the Internet of Things and cloud computing. Its outcomes are to create a new structure for secure communication among smart devices throughout the internet. Figure 1 represents the mobile ad-hoc network architecture.

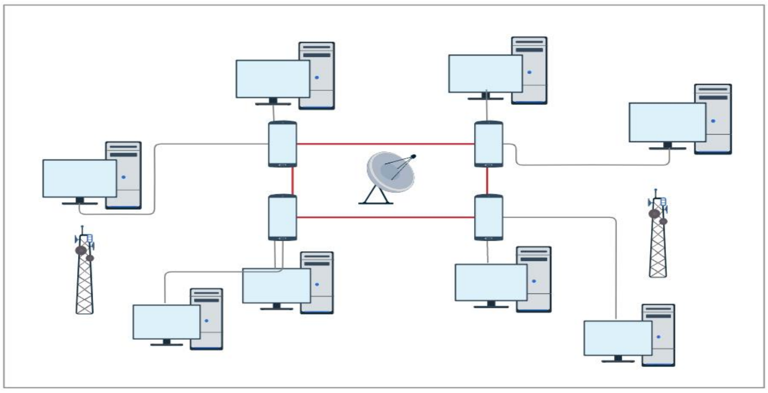

Fig. 1. MANET

[*] Corresponding author

ISSN 2443-2555 (online) 2598-6333 (print) © 2020 The Authors. Published by Universitas Airlangga.

doi: http://dx.doi.org/10.20473/jisebi.6.1.18-26

This research makes use of a desired study's correct and efficient simulation and can be implemented within an Internet of Things framework. Over the years, the field of wireless communication has been and still is growing at a rapid pace [3]. Today's most wireless network is composed of cells. The cell includes a base station, which can be connected wired or wirelessly. In the IoT framework, IoT devices provide a very useful Wi-Fi Direct feature [4]. To use this feature, any device can communicate and form a MANET [5]. When one device has internet then it can connect to the cloud and create a smart device internet [6]. When a smart device does not have enough information to selectively transmit an application, it will transmit the request to its neighboring gadgets [7]. Its most important aspect of communications is security. Starting in 2008, the rise of the IoT began by connecting the physical objects to the World Wide Web. The IoT things are connected to a big repository that has big data collection [8].

Currently, there are increasing numbers of sensors and sensor networks connected to the internet [9]. The M2M conversation is the key innovation for transferring data between transmitters [10]. There are several instruments available to turn embedded machine-to-machine communication principles into working systems [11]. Throughout a broader sense, each of the previous customers has questions about flaws in cloud computing and obstacles that might prevent them from achieving their goals.

An idea of connectivity security relies on three key points in the architecture of the internet of things.

1. Managing information from millions of sensors in a centralized smart device collection framework is not easy.
2. Managing network resources in a large network that can gather environment information from the centralized system is not an easy task.
3. Managing sensors which execute the same kind of data-parallel and stored on the centralized framework is very difficult.

The cloud has become one of the most popular paradigms in computing. Also, it came out of past computational concepts innovations that integrate parallel computation, grid computation, disseminated computation, and other computing concepts. The cloud computation provides its clients with three basic models of administration: SaaS, PaaS, and IaaS. The software as a Service (SaaS) is primarily intended for business users who need to use the software as part of their everyday practices. The platform as a service (PaaS) is primarily intended for designers of apps that need technologies to develop their software or implementation. The primary purpose of Infrastructure as a Service (IaaS) is to create network architecture [12].

When the phone network stops working, MANET communication can play a vital role to connect the smart device to each other. This really operates the devices without a phone network. These smart devices would connect to the wireless Wi-Fi network zone. All the IoT devices within the same zone can communicate with each other without a cellular network. This means interacting in a network of its own created. The own created networks are the unique network without centrally controlled, ie., MANET [13].

In the cloud-MANET framework of the internet of things, the smart device to smart device communication is a novel methodology that discovers and connects nearby smart devices without any centrally controlled resources. It will be very useful in M2M networks because there are many devices near each other in MANET. The cloud service is being used by smart device users to explore gadgets, optimize valuable information in data analysis, and store images, videos, documents, and recordings. Smart devices will be considered as IoT nodes in the proposed system [14].

MANET can be a very popular network to always get connected anywhere. The cloud provides data storage and access service. The cloud and MANET convergence offer the services for cloud access within MANET of devices connected. The group of smart device users wants to connect in a meeting at a place where there are no network services. Among smart devices, those users may form a MANET. They can also only use cloud service if one device has the internet in a group of people. In addition to its high capacity, the smart devices are currently very popular. Android devices have a new feature Wi-Fi Direct. The wireless technologies enable their users with assistance in making the very effective use of ad hoc networks for smart devices at all times and anywhere.

II. Methodologies

Connected users could communicate in cellular networks without moving through the base station, that is termed Device-to-Device communications, and can enhance bandwidth utilization. Furthermore, if it is not designed properly, D2D communication can create intervention with the current internet services. Throughout the article [15], the authors are studying an allocation of resources issue to optimize the network performance throughput when ensuring the specifications for service quality for both D2D customers and standard wireless consumers. The MANET can connect all smart devices in a decentralized approach. MANET is a self-organizing collection of mobile wireless nodes that forms a temporary network without the assistance of fixed network infrastructure or centralized approach.

Texts having a source beyond this neighborhood zone must be jumped or forwarded to the correct target address by those neighbors, who serve as routers. Figure 2 shows controlling the movements of IoT smart devices. D2D communications underpinning a cell network have been suggested as an implies of utilizing the physical connection of connecting gadgets, boosting the use of resources, and enhancing the coverage range of cellular network [16]. Usage cases for D2D could be categorized into two broad areas. First section is called peer-to-peer scenario, where the D2D gadgets are the senders and receivers for the information transferred. Second section is the scenario of the transmitter, which implies that one of the interacting D2D devices must transmit the information swapped to the node, that further forward the information to the target gadget [17]. Figure 4 represents the D2D usage cases.

Fig. 2. Controlling the movement of IoT Nodes

A. Discovering the smart devices using probability-based model

Assume that there is a MANET framework (Fig. 3) in the probability-based model. IoT nodes are functional through-axis, y-axis, and z-axis directions at the 3-dimension area. Throughout the wireless network, the whole zone is divided into cells. This zone of all cells is fixed such that the smart devices can move within cell range. IoT node will discover neighborhood devices within the same cell area in binary digits. The authorized smart device confined data that discovers the other device. The perception of the results shows that the target movement can only occur between adjacent cells. In addition, data is disseminated using a weighted normal angle and the probability of movements. The angle benefits from the simplicity of an IoT device that observes the goal spares the area of the target and sets the tilt.

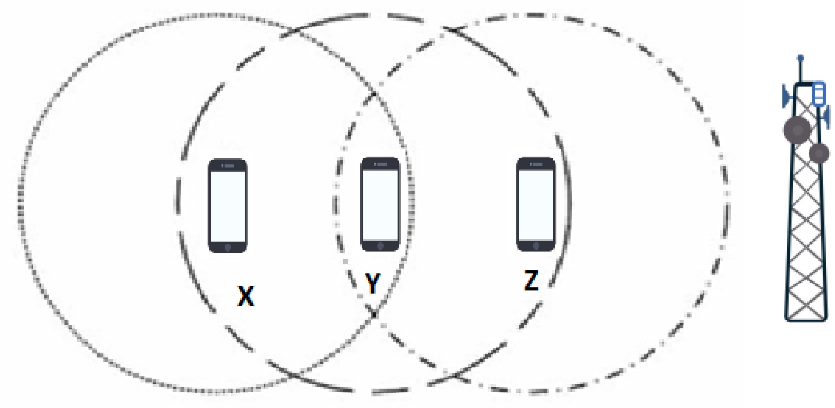

Fig. 3. MANET with three nodes

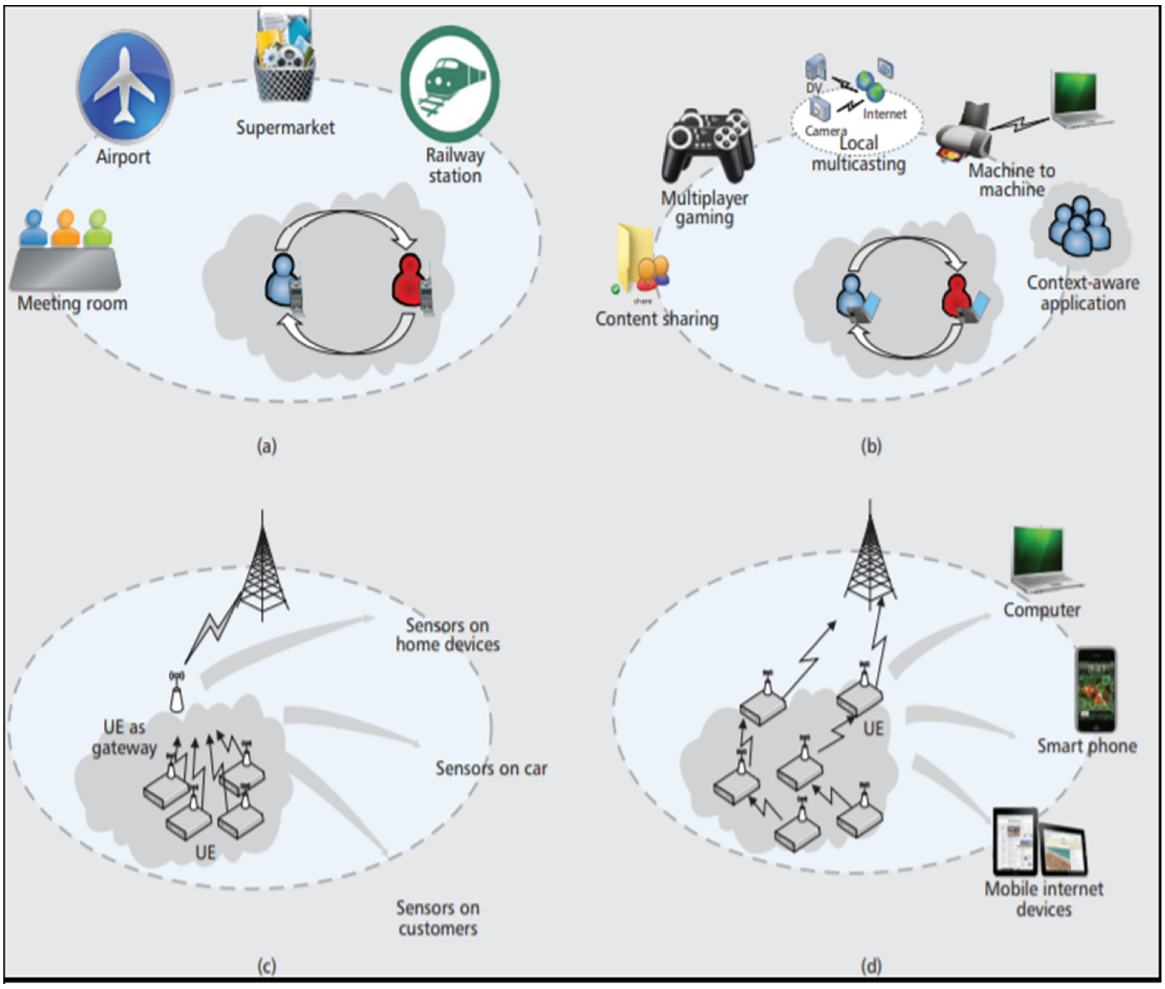

Fig. 4. D2D Usage cases [17]

B. Discovering the smart devices using hidden Markov model

The secret Markov model is used in the 2-Dimensional plane zone for discovering smart devices. The model is associated in the work area and devices are moving inside the region and this model finds within the range of neighborhood devices. Throughout the field of the wireless network, we form the transition matrix, discover all the smart devices, and place them in the transformation sequence [3].

C. Discovering the smart devices using gradient-based model

The gradient model works to identify the devices and share knowledge to create and send the information to discover the smart devices. Not by correspondence between android smart devices, but rather solely by the versatility of the Android smart device inherent in the MANET, this tendency is retained.

The gradient value set 1 will also discover android smart devices in the region where an ad hoc network is established at the point where an android smart device recognizes the target. Its gradient data is the area that has focused on going back some time. The smart device, we use an exponential decreasing capacity to continue to decrease this output as time progresses.

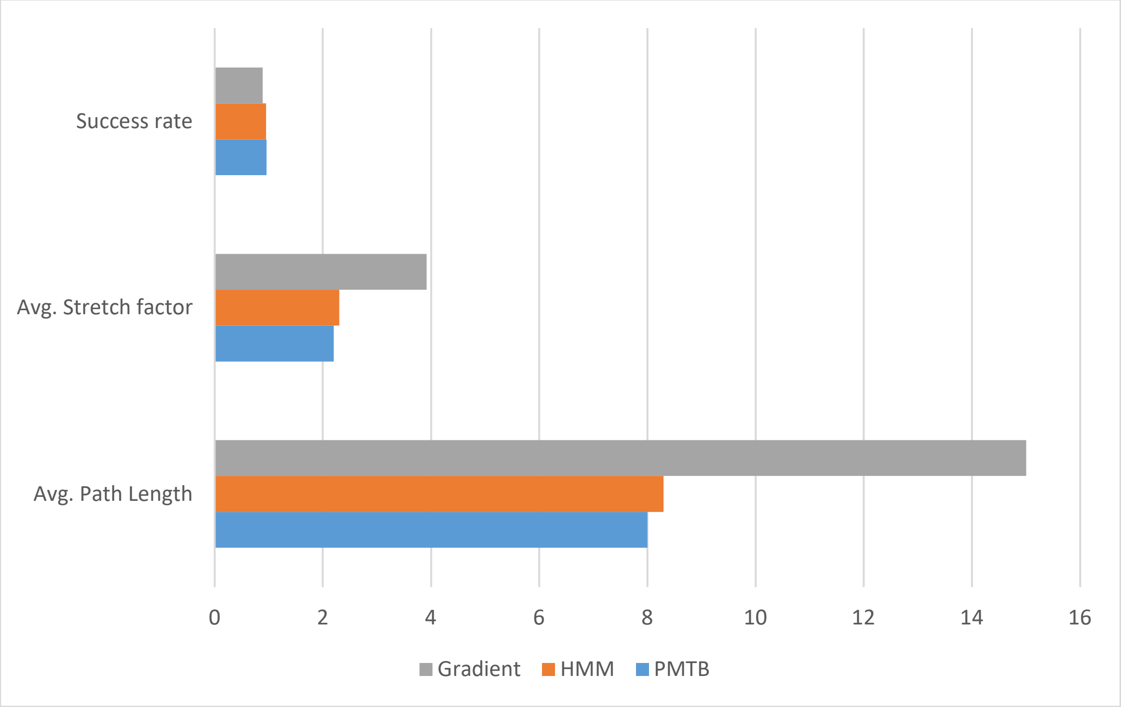

Fig. 5. PBM, HMM and gradient Model statistics [3]

Thus, the PBM model's achievement rate (Fig. 5) is best when examining HMM and Gradient Model. We, therefore, use the PBM model to outline the Ad Hoc Network among smart devices running on android [3]. The new technologies such as Wi-Fi Direct introduced by the Wi-Fi Alliance aimed at improving direct D2D communications in Wi-Fi networks [18]. Allowing D2D interaction over directional Millimeter-wave systems is crucial in using the massive bandwidth efficiently to boost data traffic [19].

III. Results

The Smart devices are positioned within the range of MANET wireless devices that accept the coverage and networking of ad hoc Wi-Fi. Each IoT device is expected to have a settled Wi-Fi zone and a changed range of correspondences. Its goal is to achieve certain requirements of the network's reach or correspondence. Fig. 6 shows the Cloud-MANET mobility model for 5G heterogeneous network. The arrangement of smart devices expressed in an objective zone, the problem is to decide whether the area is k-covered within an objective zone that is protected by Wi-Fi emphasis in any case, where k is a provided sample size. The future sixth generation mobile network is expected to be a fundamentally smart, complex, and dynamic, ultra-dense diverse network to satisfy the requirements of multiple rapidly growing apps, interconnecting all things with extraordinarily low latency and heavy-speed data distribution. Artificial Intelligence (AI) is assumed to become the most creative strategy able to achieve smart, computerized network systems, leadership, and repairs in upcoming complicated services [20].

Information and communication security is a challenge if two or even more devices wanted to communicate without the third party responding to the shared data. IoT devices are electronic devices that are connected by networking protocols such as smartphones, laptops, smart watch, etc. to all other devices or networks. MANETs allow users to communicate in an infrastructure-less network. The comprehension discussion based on the results of the D2D and cooperative communications is discussed in the paper [21].

Cloud computing allows mobile applications to share resources, storage, and services. The author focuses on the Cloud-MANET area of secure communication between smart devices. In Cloud-MANET, the smart devices are continuously connected, and a network called MANET is built on their own, and they can access cloud services. However, in this scenario, there are now more difficulties to secure communication.

MANET is a kind of wireless network that is self-organizing and auto connected in a decentralized approach. Each node in MANET can be moved freely from one location to another in any direction in the range of MANET. The IoT devices can create a MANET network with their neighbors' smart devices and forward data to another device.

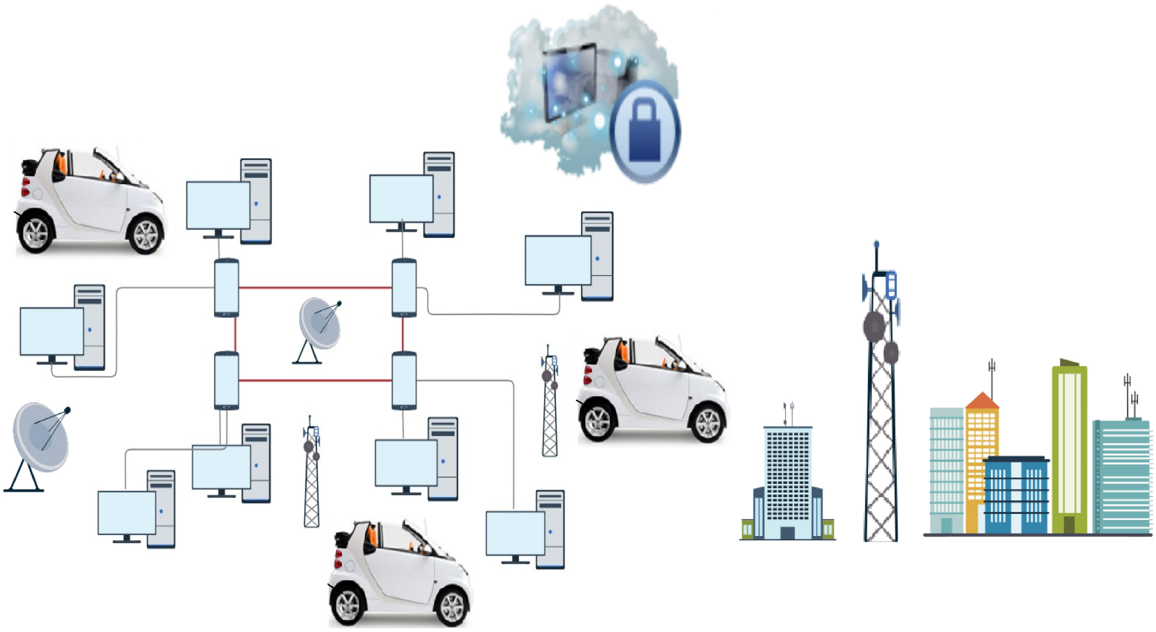

Fig. 6. Cloud-MANET model in 5G heterogeneous networks

A cloud-MANET architecture of the smart device is constructed with cloud and MANET computation. The framework allows MANET users to access and deliver cloud services through their connected devices, where all simulations, error handling, and resource management are implemented. In the area of a mobile ad-hoc network, the smart devices can move from one location to another and at least one smart device in MANET should be connected to the cloud in real-time. Discovering the neighborhood devices are shown in the thesis [22].

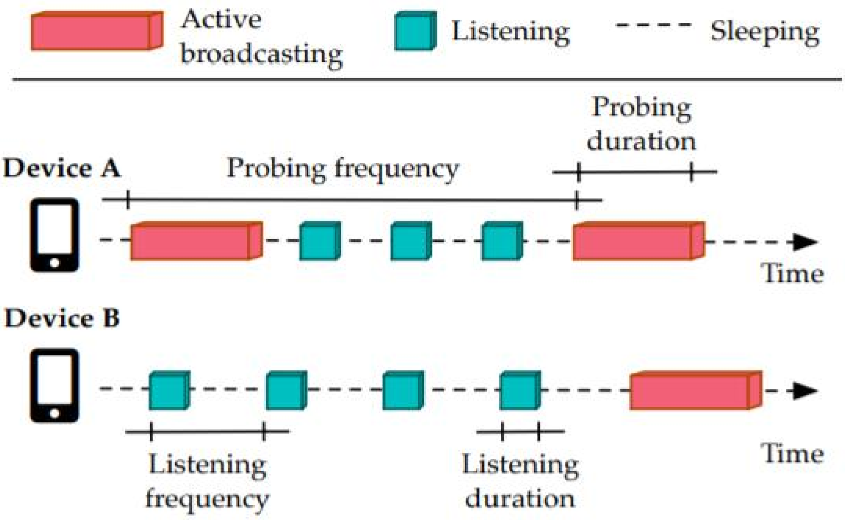

Fig. 7. Discovering Neighborhood devices [22]

The closed-form representations for the possibility of D2D termination and the possibility of confidentiality cessation are extracted [23]. D2D interaction connection is susceptible as it is relatively straightforward for allies to be undermined since D2D stations are energy restricted endpoints [24]. Different MANETs can connect to the same cloud and can use cloud service in real-time. The MANET's of smart devices need integration with mobile apps to connect to the cloud. Throughout a localized interaction, the MANET model of smart devices will operate very well using the cloud, failing while connecting in an existing wired networking environment. Through rise of IoT and 5G networks [25], the users would like to connect multiple services in a portion of secs likely to result in an additional burden on the underlying internet services to establish the arrangements on Service quality as well as Customer experience for various end-user and suppliers. The light weighted cryptographic system could be a proper solution for covering resource-constrained devices in D2D communication [26]. The efficiency of D2D communications in cache-aided structures, even though privacy restrictions are enforced on the engaging endpoints and on extrinsic snoopers [27]. The efficiency of D2D communications in cache-aided structures, even though privacy restrictions are enforced on the engaging endpoints and on extrinsic snoopers [28]. The article [29] addressed the security issues in D2D communications system. The peer discovery, relay selection and experimental prototypes developed for public safety D2D communications system are discussed in the article [30]. The author is tested the D2D communication framework in different scenarios in the cloud, MANET and IoT framework. The results are generated in the figure 8.

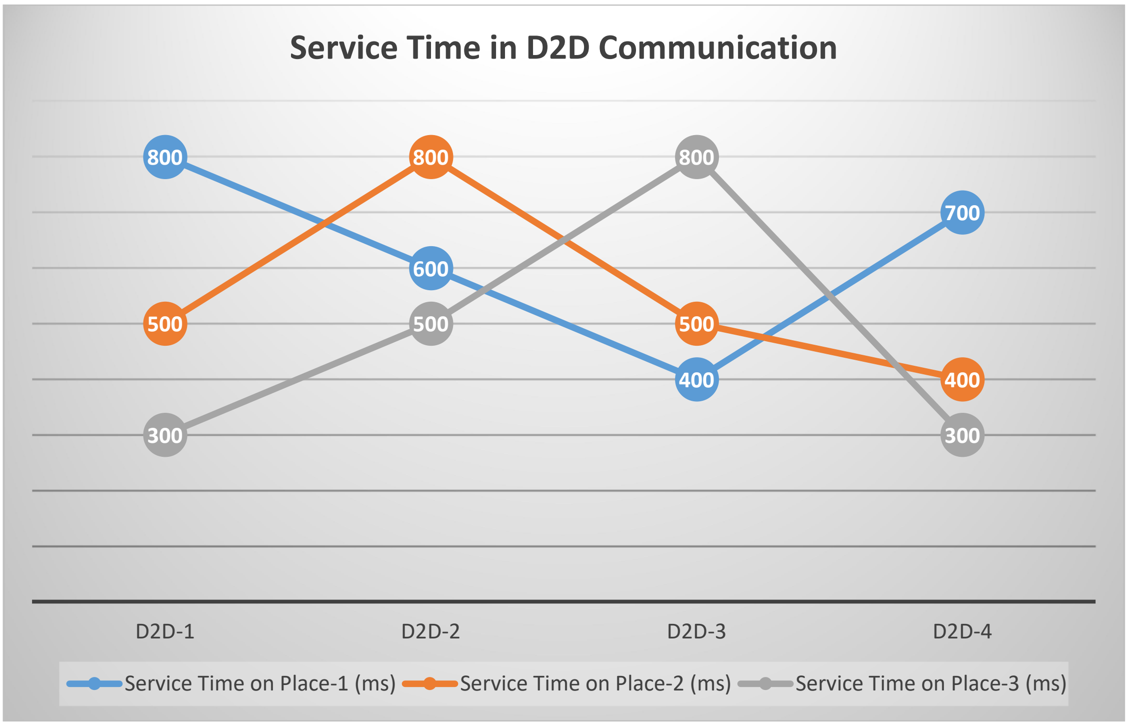

Fig. 8. Service time evaluation in D2D communication

In Figure 8, the evaluation was done in different scenarios such as in smart homes, smart labs etc. the results show the efficiency of the D2D communication. The author forms a self-created network of different IoT devices and connect to the cloud and evaluated the efficiency of the communication.

IV. Discussion

The functionality architecture for Cloud-MANET is an integrated system of Cloud Computing and MANET technologies. MANET's functionality is also dependent on its device mobility and networking tools such as storage and energy consumption. Cloud providers maintain communications infrastructure, storage facilities, and software platforms in cloud computing which support stability, effectiveness, and interoperability. MANET's smart devices can communicate with each other in the Cloud MANET convergence framework but at least one smart device must be linked to cellular or Wi-Fi connections. Every MANET IoT device should be individually registered in the cloud. This model is turned on in a disconnected style. Whenever a MANET is activated then cloud services work in real-time and provide services to MANET's smart devices. IoT devices must submit an invitation to the cloud for a networking session. The cloud provides the best IoT Device association.

V. CONCLUSIONS

The mobility model in Cloud-MANET can play the most important role in heterogeneous 5G networks. The author developed this model to improve communications efficiency and performance. Although the cloud methodology is based on a distributed framework, some of the challenges and weaknesses associated with decentralized concepts would then be inherited. Current vulnerabilities and challenges of communication security that depend on the attraction of cloud services. However, almost all those threats throughout the cloud model have intensified. The author examined the secure communication security requirements and challenges among all smart devices in cloud services environments. The MANET service has been launched as well as linked to the cloud by the mobile device. The author used the amazon cloud storage service. This research produces a conceptual model that is based on the ubiquitous method. It is shown the success in this area and expectations for future scope.

REFERENCES

[1] Militano, Leonardo, Giuseppe Araniti, Massimo Condoluci, Ivan Farris, and Antonio Iera. "Device-to-device communications for 5G internet of things." EAI Endorsed Transactions on Internet of Things 15, no. 1 (2015): 1-15.

[2] Wei, Lili, Rose Qingyang Hu, Yi Qian, and Geng Wu. "Enable device-to-device communications underlaying cellular networks: challenges and research aspects." IEEE Communications Magazine 52, no. 6 (2014): 90-96.

[3] Alam T, Benaida M. “The Role of Cloud-MANET Framework in the Internet of Things (IoT)”, International Journal of Online Engineering (iJOE). Vol. 14(12), pp. 97-111. DOI: https://doi.org/10.3991/ijoe.v14i12.8338

[4] Alam, Tanweer. "Middleware Implementation in Cloud-MANET Mobility Model for Internet of Smart Devices", International Journal of Computer Science and Network Security, 17(5), 2017. Pp. 86-94

[5] Tanweer Alam, Baha Rababah, "Convergence of MANET in Communication among Smart Devices in IoT", International Journal of Wireless and Microwave Technologies (IJWMT), Vol.9, No.2, pp. 1-10, 2019. DOI: 10.5815/ijwmt.2019.02.01

[6] Alam, Tanweer. (2018) "A reliable framework for communication in internet of smart devices using IEEE 802.15.4." ARPN Journal of Engineering and Applied Sciences 13(10), 3378-3387.

[7] Tanweer Alam, "A Reliable Communication Framework and Its Use in Internet of Things (IoT)", International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT), Volume 3, Issue 5, pp.450-456, May-June.2018 URL: http://ijsrcseit.com/CSEIT1835111.

[8] Alam, Tanweer, and Mohammed Aljohani. "Design and implementation of an Ad Hoc Network among Android smart devices." In Green Computing and Internet of Things (ICGCIoT), 2015 International Conference on, pp. 1322-1327. IEEE, 2015. DOI: https://doi.org/10.1109/ICGCIoT.2015.7380671

[9] Alam, Tanweer, and Mohammed Aljohani. "An approach to secure communication in mobile ad-hoc networks of Android devices." In 2015 International Conference on Intelligent Informatics and Biomedical Sciences (ICIIBMS), pp. 371-375. IEEE, 2015. DOI: https://doi.org/10.1109/iciibms.2015.7439466

[10] Alam, Tanweer, and Mohammed Aljohani. "Design a new middleware for communication in ad hoc network of android smart devices." In Proceedings of the Second International Conference on Information and Communication Technology for Competitive Strategies, p. 38. ACM, 2016. DOI: https://doi.org/10.1145/2905055.2905244

[11] Alam, Tanweer. "Fuzzy control based mobility framework for evaluating mobility models in MANET of smart devices." ARPN Journal of Engineering and Applied Sciences 12, no. 15 (2017): 4526-4538.

[12] Tanweer Alam, Mohamed Benaida, “Blockchain, Fog and IoT Integrated Framework: Review, Architecture and Evaluation”, Technology Reports of Kansai University, Volume - 62 , Issue 02, 2020.

[13] Tanweer Alam, “Internet of Things: A Secure Cloud-Based MANET Mobility Model”, International Journal of Network Security, Vol. 22(3), 2020.

[14] Alam, Tanweer. "A Middleware Framework between Mobility and IoT Using IEEE 802.15. 4e Sensor Networks." Jurnal Online Informatika 4, no. 2 (2020): 90-94.

[15] Feng, Daquan, Lu Lu, Yi Yuan-Wu, Geoffrey Ye Li, Gang Feng, and Shaoqian Li. "Device-to-device communications underlaying cellular networks." IEEE Transactions on communications 61, no. 8 (2013): 3541-3551.

[16] Fodor, Gábor, Erik Dahlman, Gunnar Mildh, Stefan Parkvall, Norbert Reider, György Miklós, and Zoltán Turányi. "Design aspects of network assisted device-to-device communications." IEEE Communications Magazine 50, no. 3 (2012): 170-177.

[17] Lei, Lei, Zhangdui Zhong, Chuang Lin, and Xuemin Shen. "Operator controlled device-to-device communications in LTE-advanced networks." IEEE Wireless Communications 19, no. 3 (2012): 96-104.

[18] Camps-Mur, Daniel, Andres Garcia-Saavedra, and Pablo Serrano. "Device-to-device communications with Wi-Fi Direct: overview and experimentation." IEEE wireless communications 20, no. 3 (2013): 96-104.

[19] Qiao, Jian, Xuemin Sherman Shen, Jon W. Mark, Qinghua Shen, Yejun He, and Lei Lei. "Enabling device-to-device communications in millimeter-wave 5G cellular networks." IEEE Communications Magazine 53, no. 1 (2015): 209-215.

[20] Zhang, Shangwei, Jiajia Liu, Hongzhi Guo, Mingping Qi, and Nei Kato. "Envisioning Device-to-Device Communications in 6G." IEEE Network (2020).

[21] Malik, Praveen Kumar, Deepinder Singh Wadhwa, and Jaspal Singh Khinda. "A survey of device to device and cooperative communication for the future cellular networks." International Journal of Wireless Information Networks (2020): 1-22.

[22] Álvarez, Flor. "Secure device-to-device communication for emergency response." PhD diss., Technische Universität Darmstadt, 2020.

[23] Khoshafa, Majid H., Telex MN Ngatched, Mohamed H. Ahmed, and Ahmed Ibrahim. "Secure Transmission in Wiretap Channels Using Full-Duplex Relay-Aided D2D Communications With Outdated CSI." IEEE Wireless Communications Letters (2020).

[24] Jiang, Yu'E., Liangmin Wang, Hui Zhao, and Hsiao-Hwa Chen. "Covert Communications in D2D Underlaying Cellular Networks With Power Domain NOMA." IEEE Systems Journal (2020).

[25] Prerna, Divya, Rajkumar Tekchandani, and Neeraj Kumar. "Device-to-device content caching techniques in 5G: A taxonomy, solutions, and challenges." Computer Communications (2020).

[26] Seok, Byoungjin, Jose Costa Sapalo Sicato, Tcydenova Erzhena, Canshou Xuan, Yi Pan, and Jong Hyuk Park. "Secure D2D Communication for 5G IoT Network Based on Lightweight Cryptography." Applied Sciences 10, no. 1 (2020): 217.

[27] Zewail, Ahmed A., and Aylin Yener. "Device-to-device secure coded caching." IEEE Transactions on Information Forensics and Security 15 (2019): 1513-1524.

[28] Waqas, Muhammad, Yong Niu, Yong Li, Manzoor Ahmed, Depeng Jin, Sheng Chen, and Zhu Han. "Mobility-Aware Device-to-Device Communications: Principles, Practice and Challenges." IEEE Communications Surveys & Tutorials (2019).

[29] Hamoud, Othmane Nait, Tayeb Kenaza, and Yacine Challal. "Security in device-to-device communications: a survey." IET Networks 7, no. 1 (2017): 14-22.

[30] Shah, Syed Tariq, Syed Faraz Hasan, Boon-Chong Seet, Peter Han Joo Chong, and Min Young Chung. "Device-to-device communications: A contemporary survey." Wireless Personal Communications 98, no. 1 (2018): 1247-1284.