ICN 2021

The Twentieth International Conference on Networks

ISBN: 978-1-61208-837-2

April 18 - 22, 2021

ICN 2021 Editors

Bilal Al Momani, Mohawk College of Applied Arts and Technology, Canada
Shintaro Mori. Fukuoka University, Japan
Eugen Borcoci, University Politehnica of Bucharest, Romania
Rony Kumer Saha, KDDI Research, Inc. Japan

ICN 2021

Forward

The Twentieth International Conference on Networks (ICN 2021) continued a series of events organized by and for academic, research and industrial partners.

We solicited both academic, research, and industrial contributions. We welcomed technical papers presenting research and practical results, position papers addressing the pros and cons of specific proposals, such as those being discussed in the standard fora or in industry consortia, survey papers addressing the key problems and solutions on any of the above topics short papers on work in progress, and panel proposals.

We take here the opportunity to warmly thank all the members of the ICN 2021 technical program committee, as well as all the reviewers. The creation of such a high quality conference program would not have been possible without their involvement. We also kindly thank all the authors who dedicated much of their time and effort to contribute to ICN 2021. We truly believe that, thanks to all these efforts, the final conference program consisted of top quality contributions. We also thank the members of the ICN 2021 organizing committee for their help in handling the logistics of this event.

ICN 2021 Chairs

ICN 2021 Steering Committee
Eugen Borcoci, University Politehnica of Bucharest, Romania
Pascal Lorenz, University of Haute Alsace, France
Nicola Ciulli, Nextworks, Italy
Shintaro Mori, Fukuoka University, Japan

ICN 2021 Advisory Committee
Yenumula B. Reddy, Grambling State University, USA
Eric Renault, Institut Mines-Télécom - Télécom SudParis, France
Sherali Zeadally, University of Kentucky, USA

ICN 2021 Industry/Research Advisory Committee
Marc Cheboldaeff, Deloitte Consulting GmbH, Germany
Megumi Shibuya, The University of Electro-Communications, Japan
Arslan Brömme, Vattenfall GmbH, Berlin, Germany
Cristian Anghel, Politehnica University of Bucharest, Romania / Pentalog, France

ICN 2021 Publicity Chairs
Lorena Parra, Universitat Politecnica de Valencia, Spain
Jose Luis García, Universitat Politecnica de Valencia, Spain

ICN 2021

Committee

ICN 2021 Steering Committee

Pascal Lorenz, University of Haute Alsace, France
Eugen Borcoci, University Politehnica of Bucharest, Romania
Nicola Ciulli, Nextworks, Italy
Shintaro Mori, Fukuoka University, Japan

ICN 2021 Advisory Committee

Yenumula B. Reddy, Grambling State University, USA
Eric Renault, Institut Mines-Télécom - Télécom SudParis, France
Sherali Zeadally, University of Kentucky, USA

ICN 2021 Industry/Research Advisory Committee

Marc Cheboldaeff, Deloitte Consulting GmbH, Germany
Megumi Shibuya, The University of Electro-Communications, Japan
Arslan Brömme, Vattenfall GmbH, Berlin, Germany
Cristian Anghel, Politehnica University of Bucharest, Romania / Pentalog, France

ICN 2021 Publicity Chairs

Lorena Parra, Universitat Politecnica de Valencia, Spain
Jose Luis García, Universitat Politecnica de Valencia, Spain

ICN 2021 Technical Program Committee

Luis F. Abanto-Leon, Technische Universität Darmstadt, Germany
Qammer H. Abbasi, University of Glasgow, UK
Khelil Abdelmajid, Landshut University of Applied Sciences, Germany
Alireza Abdollahpouri, University of Kurdistan, Sanandaj, Iran
Abdelmuttlib Ibrahim Abdalla Ahmed, University of Malaya, Malaysia
Ahmedin Mohammed Ahmed, FDRE Ministry of Innovation and Technology (MInT), Ethiopia
Francisco Airton Silva, Federal University of Piauí, Brazil
Sami Marzook Alesawi, King Abdulaziz University | Faculty of Computing and Information Technology at Rabigh, Saudi Arabia
Madyan Alsenwi, Kyung Hee University - Global Campus, South Korea
Reem Alshahrani, Kent State University, USA
Cristian Anghel, Politehnica University of Bucharest, Romania / Pentalog, France
Imran Shafique Ansari, University of Glasgow, Scotland, UK
Andrés Arcia-Moret, Xilinx, Cambridge, UK

Copyright Information

For your reference, this is the text governing the copyright release for material published by IARIA.

The copyright release is a transfer of publication rights, which allows IARIA and its partners to drive the dissemination of the published material. This allows IARIA to give articles increased visibility via distribution, inclusion in libraries, and arrangements for submission to indexes.

I, the undersigned, declare that the article is original, and that I represent the authors of this article in the copyright release matters. If this work has been done as work-for-hire, I have obtained all necessary clearances to execute a copyright release. I hereby irrevocably transfer exclusive copyright for this material to IARIA. I give IARIA permission or reproduce the work in any media format such as, but not limited to, print, digital, or electronic. I give IARIA permission to distribute the materials without restriction to any institutions or individuals. I give IARIA permission to submit the work for inclusion in article repositories as IARIA sees fit.

I, the undersigned, declare that to the best of my knowledge, the article is does not contain libelous or otherwise unlawful contents or invading the right of privacy or infringing on a proprietary right.

Following the copyright release, any circulated version of the article must bear the copyright notice and any header and footer information that IARIA applies to the published article.

IARIA grants royalty-free permission to the authors to disseminate the work, under the above provisions, for any academic, commercial, or industrial use. IARIA grants royalty-free permission to any individuals or institutions to make the article available electronically, online, or in print.

IARIA acknowledges that rights to any algorithm, process, procedure, apparatus, or articles of manufacture remain with the authors and their employers.

I, the undersigned, understand that IARIA will not be liable, in contract, tort (including, without limitation, negligence), pre-contract or other representations (other than fraudulent misrepresentations) or otherwise in connection with the publication of my work.

Exception to the above is made for work-for-hire performed while employed by the government. In that case, copyright to the material remains with the said government. The rightful owners (authors and government entity) grant unlimited and unrestricted permission to IARIA, IARIA's contractors, and IARIA's partners to further distribute the work.

Table of Contents

Assessing the Performance of Mobile Ad-Hoc Network (MANET) Routing Protocols

Bilal Al Momani
Electrical and Computer Engineering Technology
Mohawk College of Applied Arts and Technology
Hamilton (ON), Canada
e-mail: bilal.al-momani@mohawkcollege.ca

Esteve Hassan
Electrical and Computer Engineering Technology
Mohawk College of Applied Arts and Technology
Hamilton (ON), Canada
e-mail: esteve.hassan@mohawkcollege.ca

***Abstract* — This paper focuses on evaluating some of the routing protocols for the Mobile Ad-Hoc Network (MANET) and discusses their abilities to provide advanced Quality of Service (QoS) support in spite of their dynamic nature. Two routing protocols have been extracted to be studied extensively and compared against each other in terms of their performance: the on-demand Dynamic Source Routing (DSR) along with the table-driven Destination-Sequenced Victor (DSDV) routing protocol. The performances are analyzed according to various factors such as network load, mobility, and network size using a set of parameters. The evaluation shows that an on-demand routing protocol is preferable in all routing conditions.**

Keywords: MANET; Routing Protocols; Packet Delivery Fraction Ratio; Normalized Routing Load.

I. INTRODUCTION

The increased importance of wireless networks is increasingly evident since the demand to access information from any part of the globe has overwhelmed supply. Reduction in cost and time taken to build wired infrastructure has become the ultimate objective for networks designers. Wireless networks can be classified into two categories: “infrastructure” networks and “Infrastructureless” networks. Infrastructure networks usually have fixed and wired gateways and mobile nodes communicate with the network through a base station. The mobile nodes can continue communication with the network even if out of range by connecting with a new fixed base station or access point. The other classification of networks is Infrastructureless, also known as ad-hoc networks. This type of network has no fixed infrastructure or routers; all nodes within the network are mobile and able to move freely to different locations, they can connect dynamically in an arbitrary manner. Each node within ad-hoc network acts as a host and router at the same time. Fig. 1 gives a simplified overview of an ad-hoc network. This figure shows how different heterogeneous hosts are communicating without any infrastructure (Soldiers, tanks, vehicles, satellites).

The biggest problem facing the ad-hoc networks is that it consists of wireless hosts, which have the ability to move in an unpredictable fashion. The movement of these nodes creates many complex issues resulting in changes in routes and addresses, which requires some new mechanisms for planning suitable routing protocols and other configurations.

So far, network simulations, using simulation software, have been done on both the DSR and DSDV protocols and the results have been taken. Results have shown that the on-demand routing protocols are more efficient in solving the routing problem in a mobile environment than the table-driven protocols. Therefore, the comparison between the ad-hoc protocols is a continuous concern, due to the importance of these protocols in a wireless world.

The objective of this work is to undertake the most important issues regarding ad-hoc networks, evaluate their performance based on their properties and their ability to provide QoS and follow with an overview comparison between some selected protocols. Simulation environments are used to compare the performance of DSR and DSDV to examine the impact of the mobility of nodes on the behavior of these protocols regarding packet delivery, delay and routing load. The simulation results show that DSR outperforms DSDV in select scenarios.

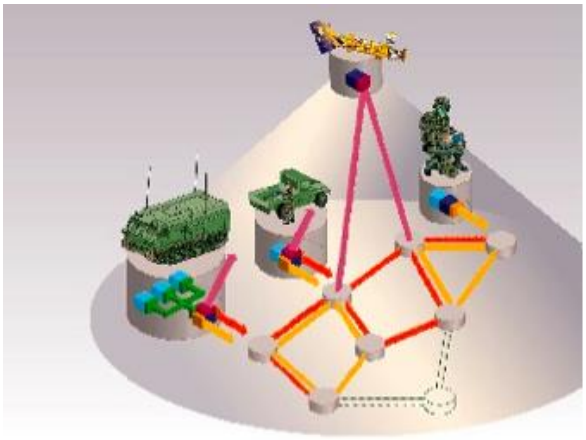


Figure 1. A simplified overview of MANET

The rest of this paper is organized as follows. Section II addresses some related study. Section III describes the MANET routing protocols in general, and then specifically describes the two main protocols under comparison; DSR and DSDV. Section IV introduces the simulation environment.

 ISBN: 978-1-61208-837-2

Section V discusses the simulation results. Section VI outlines the conclusion of this paper.

II. RELATED WORK

Due to the importance of ad-hoc wireless networks, many routing protocols have been proposed and developed. Each one of these protocols has been designed for special applications. Therefore, differences between them are a point of contention.

Continued work on performance evaluation and comparisons between ad-hoc routing protocols has been conducted by different researchers, using different methods of evaluation, such as simulations, algorithms, and mathematical analyses. In one study, a comparison between different types of protocols in term of control traffic overhead and loop-free properties based on theoretical analysis and discussion is made [1]. Other comparisons between the main categories of ad-hoc protocols have taken place based on Quality of Service [2]. Another study used simulations to compare three ad-hoc protocols [3]. Multiple studies comparing the performance between three ad-hoc protocols have also been done, with the performance comparison as their main issue [4], [5].

III. MANET ROUTING PROTOCOLS

Routing is a process of forwarding packets from source to destination; the path from source to destination should meet the QoS requirements such as: packet delay, delay jitter, bandwidth and packet loss [6]. The dynamic nature of the nodes in an ad-hoc network makes it difficult to sustain the precise link information that meets the QoS routing. Some of the MANET protocols properties, such as dynamic topology, multiple wireless links, physical security, power constrained, and limited resources heighten the pressure on routing protocols that can adapt with these characteristics, which are not met by traditional routing protocols [7],[8]. Therefore, the need for special routing protocols with certain properties is highly essential to meet the ad-hoc nature. Some desired characteristics of these protocols are: distributed, on demand operations, secure, loop free, bi-directional/uni-directional, QoS, energy and bandwidth reservation, and entering/departing nodes [9]. To meet the desirable properties above, many protocols have been proposed by the IETF MANET group [10] for the ad-hoc networks. These protocols can be classified into the following categories: table-driven, on-demands and hybrid protocols [11]. Table 1 shows general differences between on-demand and table-driven based routing protocols as stated in [12].

Table-driven, also called proactive, protocols are based on updating the information in the routing table periodically. This will enable the ad-hoc node to operate in steady fashion and up-to-date routing table. These protocols identify the network topology before any forward packet happens. Examples of these protocols are Destination-Sequenced Distance Vector (DSDV), Wireless Routing Protocol (WRP) and Source Tree Adaptive Routing (STAR) [13].

On-demand, also called reactive, protocols, a complete routing table is not required; Instead, hosts establish routes when they need that. Examples of these protocols are: AODV (Ad-hoc On-Demand Distance Vector protocol), DSR (Dynamic Source Routing Protocol), TORA (Temporally Order Routing Algorithm) and ABR (Associated Based Routing). For this study, the DSR and DSDV from each type were selected for further discussion, analysis and performance evaluation. These protocols have been used for different applications ranging from small networks with low mobility, to large networks with high mobility. None of these protocols is suitable for the whole ad-hoc application; each one has its own characteristics to suit a specific application.

TABLE 1. GENERAL DIFFERENCES BETWEEN ON-DEMAND AND TABLE-DRIVEN

Parameters	On-demand	Table-driven
Availability of Routing Information	Available when needed	Always available regardless of need
Routing Philosophy	Flat	Mostly flat
Periodic Rout update	Not required	Required
Coping with mobility	Using localized route discovery	Inform other nodes to achieve consistent routing table
Signalling traffic generated	Grown with increasing mobility of active routes as in ABR	Greater than that of on-demand routing
Quality of Service	Some can support QoS	Mainly Shortest Path as QoS metric

A. DSR

DSR [14] is an on-demand routing protocol. It uses the source routing mechanism to discover routes. The sender knows the complete route (hop-by-hop) to the destination. These routes are stored in a route cache and the data packet carry the source route are in the packet header.

As seen in Fig. 2, Node A is discovering a route to node D. Each node forwards the *ROUTE REQUEST* from A, adding its own address to the list in the packet; the combination of the initiator address (A), the target address (D), and the request identifier (2) assigned by node A uniquely identifies this Route Discovery [15].

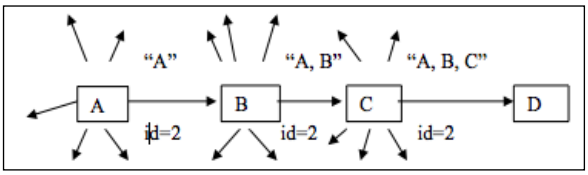


Figure 2. Route Discovery in DSR

B. DSDV

DSDV [16] is a table-driven routing protocol that has been designed to ad-hoc networks as a modification to Bellman-Ford algorithm [17].

It is a hop-by-hop distance vector routing that requires every node to continually broadcast routing updates. Each node maintains a routing table. This routing table contains the next hop to be accessed from this node, and the distance to that hop. Each route in the routing table is marked with a sequence number that reflects the freshness of the route [16]. This sequence number is originated at the destination node. Whenever an update is required, each node broadcasts an increasing sequence number for itself to all of its neighbors. When a node adjusts a route, it broadcasts an update with a sequence number greater than its sequence number for that route [16]. When a node receives a limitlessness metric with a later sequence number, it will prompt a route update broadcast to disseminate the news. The DSDV then, updates routes when faces a route failure as shown in Fig. 3.

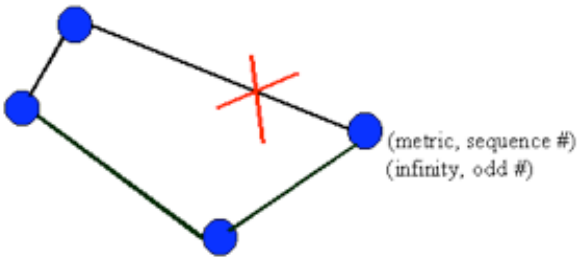


Figure 3. DSDV updates routes when faces a route failure

The above two protocols' performance are then assessed using the Network Simulator tool with predefined performance metrics as explained below.

IV. SIMULATION ENVIRONEMNT

In this study, the Network Simulator (ns-2) from Berkley was used [18]. Fig. 4 shows a simplified user's view of NS. This figure shows that for C++ objects that have an OTcl linkage forming a hierarchy, there is a matching OTcl object hierarchy very similar to that of C++ [18]. This simulation is used to study a performance comparison between the two ad-hoc protocols (DSDV and DSR). The simulation models all the control message exchanges at the MAC layer and network layer.

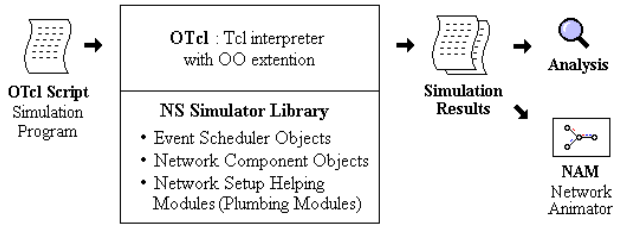


Figure 4. Simplified overview of NS

C. Simulation Setup and Parameters

The IEEE 802.11 at 2 Mbps was used in this simulation as physical, data link, and MAC layer protocols. The *random way-point* was used as the mobility model. The area used is 600m X 600m with fixed 50 nodes. The maximum speed for the mobile node is 20 m/s (0-20m/s). 20 sources are used, each source sends four 512-byte data packets per networks. Complete setup is explained in the simulation parameters in in Table 2 below. These parameters are used for both protocols (DSR and DSDV).

TABLE 2. SIMULATION PARAMETERS

Total Number of Nodes	50
Size of simulation area	600m X 600m
Movement model used	Random way-point
Pause time used	0, 10, 20, 40, 100, 200 seconds
Total simulation time	200 sec
Traffic type	CBR (Constant (Continuous) bit rate
Packet size	512 bytes
Data rate	4 packets/second
Interface queue size	50 packets
Nodes movement speed	0-20m\s
Ratio model used	Lucent's wave LAN
MAC protocol	IEEE 802.11 distribute coordination function (DCF)
Send buffer	64 packets
Type of link	Bi-directional

As shown in above table, the parameters used in this simulation are:

- Total number of nodes. 50 nodes.
- Size of simulation. 600m X 600m.
- Movement Model used. The mobility model used for the nodes is the "random way-point" model [19]. In this model, the movements of mobile nodes are broken into repeating pause and motion period. A mobile node first stays at a location for a certain time then it moves to a new random-chosen destination a speed uniformly distributed between [0, max speed]. Here, each packet starts its movement from a random location to a random destination with a random chosen speed (0-20m\s). Once the destination is reached, another random destination is targeted after a pause.
- Pause time: the time a node stays at a position before moving to the next random position. Different pause times were used in this simulation 0,10,20,40,100, and 200 seconds. A 0-second pause time indicates that nodes are continuously moving while a 200-second

 ISBN: 978-1-61208-837-2

pause time means that nodes are at rest for the entire simulation.

- Total simulation time. In this simulation a 200 seconds total simulation time is used.
- Traffic type. Constant (Continuous) bit rate (CBR) traffic sources are used in this simulation with packet size 512 bytes and packet sending rate in each pair is set to 4 packets / second. The CBR is used as traffic here and not the TCP because the main object is to evaluate the performance of the two protocols to see how they behave toward the selected metrics.
- Interface queue size. The interface queue has a maximum size of 50 packets. It is a drop-tail priority queue with two priorities each served in FIFO.
- Nodes movement speed. Nodes move at speeds between 0 and 20m\sec.
- Radio model used. The ratio model uses characteristics similar to the radio interface, Lucent's WaveLAN card. WaveLAN is modelled as a shared-media with nominal bit rate of 2Mb\s and a nominal ratio range of 250m.
- MAC protocol. The distribution coordination function (DCF) of IEEE 802.11 for WLAN is used as the MAC layer protocol; with unslotted carrier senses multiple access techniques with collision avoidance (CSMA\CA).
- Send buffer. The protocols maintain a send buffer of 64 packets. That means network layer a 64 packets send buffer is used for storing packets waiting for routing, such as packets for which route discovery has started, but no reply has arrived yet.
- Bi-Directional link. Each node sends data to other nodes and visa versa.

D. Performance Metrics

There are several metrics that can be used to assess the routing protocols. In this simulation the following metrics are used to assess the performance of the two routing protocols [15].

- *Packet Delivery Fraction (PDF)*. The fraction of originated data packets that are successfully delivered to their planned destination nodes. This metric is most important for best-efforts traffic. This can be calculated from the following formula:

$$PDF = (received\ packets \setminus sent\ packets) * 100 \quad (1)$$

- *Average end –to–end delay*. This includes all possible delays caused by buffering during route discovery latency, queuing at the interface queue, retransmission delays at MAC, and propagation, and transfer times. It can be derived from the formula:

$$Average\ End\text{-}to\text{-}end\ delay = (time\ pkts\ received\ destination) - (time\ the\ pkts\ generated) \quad (2)$$

- *Normalized routing load (NRL)*. The number of routing packets transmitted per data packets delivered at the destination. Each hop-wise transmission of routing packet is counted as one transmission. It is the total number of overhead packets used by the routing protocol (DSDV / DSR). The formula used to evaluate this metric is:

$$NRL = routing\ packet\ sent/\ received \quad (3)$$

E. Methodology

Fig. 5 is an overview of the implementation and simulation design used starting from writing the script, generating the required scenarios and then getting the simulation output. This figure shows that, main OTcl application script is used to connect all components together to complete the simulation.

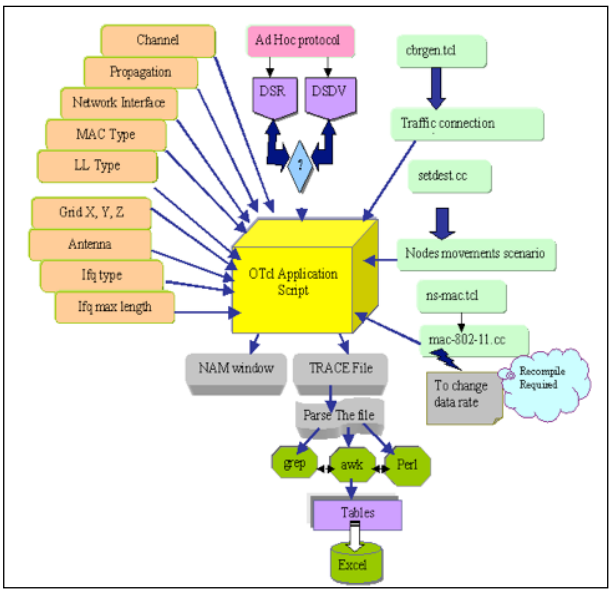


Figure 5. Simulation design overview

The OTcl script is used to setup the network configuration and components, the nodes links, send data between the nodes, etc. Fig. 6 shows the script used to define the network model components. This part o fthe script defines how the mobile nodes are configured. Communication between mobile nodes generates a necessity for a random traffic connection. Either TCP or CBR can be setup between mobile nodes using a traffic-scenario generator script. This script is used to generate CBR and TCP traffics connections between mobile nodes. So, we define the type of traffic (CBR or TCP), the number of nodes, the maximum number of connections to be setup between them, a random seed and in case of CBR connections, a rate whose inverse value is used to compute the interval time between the CBR packets. CBR connection file is created between 50 nodes having maximum connection of 20 connections, with a seed value 1.0 and a rate 4.0.

```
set val(prop)      Propagation/TwoRayGround          ;# channel type
set val(netif)     Phy/WirelesTPhy          ;# radio propagation model
set val(mac)       Mac/802_11                              ;# mac type
set val(ifq)Queue/DropTail/PriQueue          ;#Interface queue type
set val(ll)        LL                                    ;#Link layer type
set val(ant)       Antenna/OmniAntenna                   ;#Antenna type
set val(x)         600                ;# X dimension of the topography
set val(y)         600                ;# Y dimension of the topography

set val(ifqlen)              50                    ;# max packet in ifq
set val(seed)               0.0                      ;# the seed value
set val(tr)         tracefile.tr                     ;# trace fil

set val(nm)              tracenam.nam      ;# the nam for visualization

set val(adhocRouting)      DSDV|DSR    ;#the ad-hoc protocol used
set val(nn)                  50                    ;# simulated nodes
set val(cp)       "../scenarios/cbr-50-5-4"              ;# the traffic
connection file generated

set val(sc)       "../scenarios/scen-50-20-0”      ; # the scenario file
generated

set val(stop)            200.0                     ;# simulation time
```

Figure 6. Mobile Node Configuration in Otcl

The Otcl script is also used to create Traffic connection either TCP or CBR and node movement. – *Not shown here due to space limitations.*

F. Analyizng the simulation output

The simulation results can be analyzed using the two methods, the NAM file, and the trace file. The NAM file is used to visualize the simulation output as shown in Fig. 7. The trace file needs to be parsed in order to extract the required information.

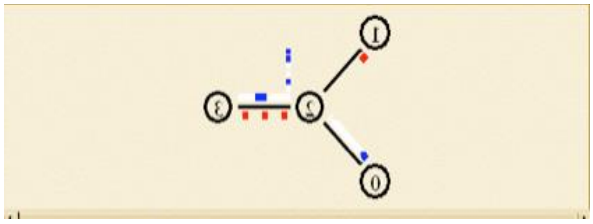
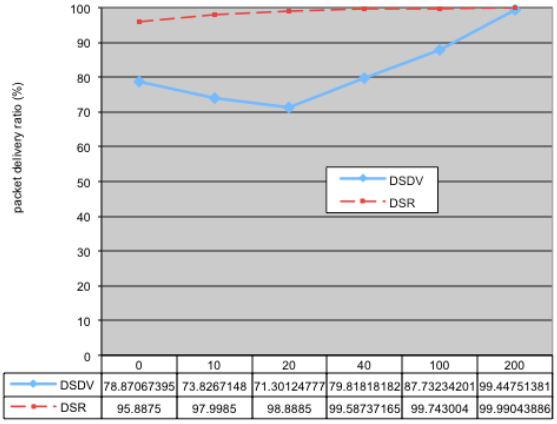


Figure 7. The NAM window

G. Packet Delivary Fracton Ratio

Fig. 8 shows the PDF for the two protocols after plotting the data from the trace files generated. From this figure, it is clear that DSR performed better than DSDV. In DSR most of the originated data was delivered successfully even when the mobility is high, more than 95% of data was delivered effectively.

Fig 8 shows that, DSDV has shown to lack productivity; almost 77% of packets were delivered, that means it has dropped around 23% of data generated. So, when mobility is high (pause time is 0 seconds), DSR outperformed DSDV with number of data delivered from the total that originated.



	0	10	20	40	100	200
DSDV	78.87067395	73.8267148	71.30124777	79.81818182	87.73234201	99.44751381
DSR	95.8875	97.9985	98.8885	99.58737165	99.743004	99.99043886

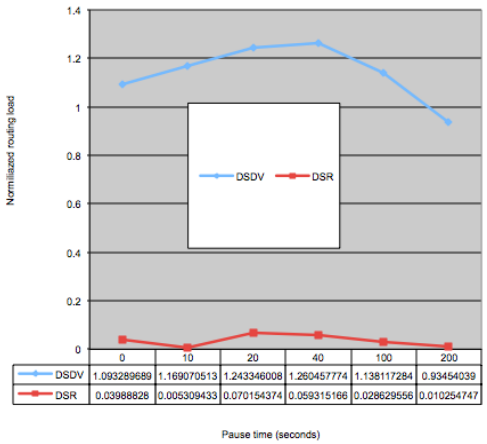
Figure 8. Packet Delivery Ratio

When the pause time is 200 second (the nodes are not moving), both protocols performed well almost all of the generated data has been delivered successfully for DSR and DSDV.

H. Normalized Routing Load

As shown in Fig. 9, there was a significant low routing load for the DSR regardless of mobility. It is fluctuating between 0.01 and 0.07; the highest routing load for DSR was when pause time is 20 seconds (medium mobility), and the lowest when pause time is 200 seconds (no mobility). Overall, DSR has a low routing load in all cases.

DSDV recorded higher routing load routing from 0.93 to 1.26. The highest routing load achieved when pause time is 40 seconds (moderate mobility), and the lowest when mobility is high (pause time is 0).



	0	10	20	40	100	200
DSDV	1.093289689	1.169070513	1.243346008	1.260457774	1.138117284	0.93454039
DSR	0.03988828	0.005309433	0.070154374	0.059315166	0.028629556	0.010254747

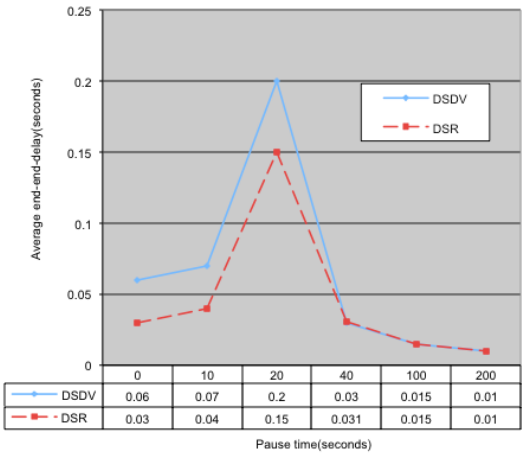
Figure 9. Normalized Routing Load

Overall, DSR outperforms the DSDV, since it has lower routing load. The reasons for these readings will be discussed in the next section.

 ISBN: 978-1-61208-837-2

I. *End –to-End Delay*

The average end-to-end delay is higher in case of DSDV. The DSR protocol outperform the DSDV in all mobility cases as shown in Fig. 10, it however is not a big difference, when the mobility is the highest (0second pause time), the delay on DSR is, almost, 0.03 seconds, and for DSDV 0.05 seconds.



	0	10	20	40	100	200
DSDV	0.06	0.07	0.2	0.03	0.015	0.01
DSR	0.03	0.04	0.15	0.031	0.015	0.01

Figure 10. End-to-End Delay

This delay increases with decreasing the mobility to reach the highest for both protocols when the pause time 20 seconds. Still, at this stage DSR performs better. This increasing of average delay goes down again with decreasing mobility when pause time equals 40 sec. Until the end of pause time 100, and 200 seconds, both protocols, almost behave the same. The minimum delay was recorded when the mobility reached the lowest level (pause time is 200 seconds). In this case, both protocols performed well.

V. RESULTS AND DISCUSION

The same simulation model was used for both protocols, in order to compare the two protocols under the same circumstances to evaluate their behavior. The main objective is to evaluate the performance of those two protocols when changing mobility. Therefore, the same movement model was used. The number of nodes is set to 50, the maximum speed was set to 20m/s, and the pause time was varied between 0, 10,20,40,100, and 200 seconds. Varying the pause time will put the two protocols in different mobility conditions. The 0 seconds pause time means the highest mobility, while the 200 seconds pause time is the lowest (no motion).

After recording the results from the simulation, many observations may be identified.

The different mechanisms that the two routing protocols use to discover the route, affect their performance. The higher the mobility the more link failure occurs within the network. Therefore, a different reaction from both protocols will be used to deal with this failure. When no mobility (pause time is 200 seconds), both protocols performed well regarding the successful data delivered from the original. Whereas, when mobility is high (pause time is 0), DSDV performed poorly, and almost a quarter of the generated packets were dropped. The reason for the high number of dropped packets in DSDV is due to the mechanism that DSDV uses to build the routes.

As explained above, each node maintains a routing table for the whole network. Therefore, the dropped packets result from stalling the routing table's entry that directed and forwarded them over a broken link. In addition, the idea of DSDV having only one route for a specific destination with no alternative caused the MAC layer to drop the packets that were not delivered. This is because the route is broken, and no alternative is available.

The DSR performed well in all cases. Even with high mobility (pause time is 0), more than 95% of originated packets were delivered. In all mobility cases, between 96% and 100% of packets were delivered.

There is a notable difference between the two routing protocols regarding the average end-to-end delay time. In all cases, DSR performed better than DSDV. As mentioned before, the DSDV uses the table-driven approach to maintain the routing information. Therefore, to be able to adapt with updating these routing tables after any route changes, extra time is needed, causing a time delay. In contrast, DSR uses an on-demand approach that builds the route whenever needed. This makes it more adaptive to any routing changes, causing less time delay.

In case of normalized routing load, DSR performed very well and had lower routing load in all cases than DSDV. The reason is that DSR uses the cache routing strategy which means the route can be found in the route cache without the need for route discovery, so it is more likely to find the route within the cache than the routing table.

VI. CONCLUSION

A comparison has been made between two mobile ad-hoc routing protocols, DSDV (table-driven), and DSR (on-demand). The Network Simulator (ns2) was used in these simulations to evaluate the performance of these two protocols. Similar parameters were set for both protocols to evaluate their behaviors under the same conditions toward mobility.

The on-demand routing protocol, DSR, outperformed the table-driven protocol, DSDV, in all chosen metrics. In addition, DSR protocol uses the route cache mechanism to discover routes and *doesn't depend on any timer-based activity*. In addition, DSR uses two routes per destination. If the protocol faces any broken links in one of the routes, an alternative path for the route is already available. The only limitations that DSR has is that it employs an aggressive use of caching, and a lack of any mechanism to expire state routes or determine the freshness of routes when multiple choices are available. DSDV is a suitable protocol in cases of low mobility and no continuous changing of topology. In addition, it is the right solution when the network is small.

 ISBN: 978-1-61208-837-2

The main conclusion that can be drawn from this evaluation is that on-demand routing protocols perform better than the table-driven protocols for the mobile ad-hoc networks. However, the main challenge in the ad-hoc network environment is designing a special mobile ad-hoc routing protocol that can deal with the heterogeneity of network resources, and be able to select routes based on the requirements of each node, to achieve a high scalability within the ad-hoc world. Therefore, comparison between these protocols is still a principal issue of researches. However, there are other research issues related to MANET still undergoing such as security, address auto-configuration and scalability that can be proposed as future work for this study.

REFERENCES

[1] C. Wahi and S. Sonbhadra, " Mobile Ad-hoc Network Routing Protocols: A Comparative Study," International Journal of Ad-hoc, Sensor & Ubiquities Computing, Vol. 3, No. 2, pp. 21-32, April 2012.

[2] X. Hong, K. Xu, and M. Gerla, "Scalable routing protocols for mobile ad-hoc networks," in IEEE Network, vol. 16, No. 4, pp. 11-21, August. 2002

[3] A. K. S. Ali and U. V. Kulkarni, "Comparing and Analyzing Reactive Routing Protocols (AODV, DSR and TORA) in QoS of MANET," IEEE 7th International Advance Computing Conference (IACC), pp. 345-34, January 2017.

[4] S. -. Lee and M. Gerla, "Dynamic load-aware routing in ad hoc networks," ICC 2001. IEEE International Conference on Communications. Conference Record (Cat. No.01CH37240), Helsinki, Finland, 2001, pp. 3206-3210 vol.10, doi: 10.1109/ICC.2001.937263.

[5] H. Jiang and J. Garcia-Luna-Aceves, "Performance comparison of three routing protocols for ad-hoc networks," Proceedings Tenth International Conference on Computer Communications and Networks , pp. 547-554, 2001.

[6] M. T. Sultan and S. M. Malik," Evaluation of Energy Consumption of Reactive and Proactive Routing Protocols in MANET", International Journal of Computer Networks & Communications, Vol. 9, No. 2, pp. 29-38, March 2017.

[7] L. E. Miller and X. Pallot, "Implementing message priority policies overan 802.11 based mobile ad-hoc network," IEEE MILCOM 2001, pp. 861–865, October 2001.

[8] S. Corson and J. Macker, "Mobile Ad-hoc networking (MANET) Routing Protocol Issues and Evaluation Considerations," Internet draft RFC 2501, 1999.

[9] A. Burjari, C. Calafate, J. Cano, P. Manzoni, C. Palazzi , and D. Ronazani, "Flaying ad-hoc network application scenarios and mobility models," International of Distiributed Sensor Networks, Vol 13, No. 10, pp. 1- 17, Sepetember 2017.

[10] The IETF manet Group. http://www.ietf.org/html.charters/manet-charter.html, retreived March, 2021.

[11] J. Song and L. E. Miller, " Empirical Analysis of the Mobility Factor for the Random Waypoint Model", Wireless Communications technologies Groups, 2002.

[12] E. M. Royer and CK Toh," A Review of current Routing Protocol for Ad-hoc mobile wireless Networks, " IEEE Personal Communicatioons, April 1999.

[13] J. L. Sobrinho and A. S. Krishnakumar, "Quality-of-Service in Ad-hoc Carrier Sense Multiple Access Wireless Networks, " IEEE Journal on Selected Areas in Communications, Vol. 17, No. 8, pp. 1353-1368, August 1999.

[14] T-W. Chen, J. T Sai, and M. Gerla, "QoS Routing Performance in Multihop, Multimedia, Wireless networks, " Proceeeding of the I6th IEEE International Conference on Univerals Personal Communications, October 1997.

[15] Y-C. HU and D. B. Johnson, "Ensuring cache freshness in on-Demand Ad-hoc network routing protocols," POMC '02: Proceedings of the second ACM international workshop on Principles of mobile computing, Oct. 2002, pp. 25-30.

[16] J. Jacob and V. Seethalakshmi, "Performance Evaluation of Various Routing Protocols in MANET, " International Journal Of Engineering Science, vol. 5, pp. 208-220, 2011.

[17] A. S. Tanenbaum, " Computer Networks", third edition, Englewood Cliff, NJ: Prentice Hall, 1996.

[18] The Network Simulator- ns2, http://www.isi.edo/nsnam/ns/ , retrieved March, 2021.

[19] A .P. Singh, A. K. Shukla and A. Mishar," Movement Evaluation of Mobilty Models in Ad-hoc Networks," International Journal of Engineering Trends and Techniology, Vol.11, No. 9, pp. 417-421, May 2014.

 ISBN: 978-1-61208-837-2

A Fundamental Analysis of an Erase Code-enabled Data Caching Scheme for Future UAV-IC-WSNs

Shintaro Mori
Department of Electronics Engineering and Computer Science
Fukuoka University
8-19-1, Nanakuma, Jonan-ku, Fukuoka 814-0180, Japan
e-mail: smori@fukuoka-u.ac.jp

***Abstract*—This paper addresses an effective scheme for sensing data collection and management in future smart city applications for rapid urbanization. The main contribution of this paper provides an application of Internet of things as a new Internet technology as case study. In particular, we focus on two key technologies, an information-centric network and unmanned aerial vehicles. We propose a novel joint sensing, forwarding, and storing scheme, for which we introduce an erase code technique and cross-layer optimization. We provide the overall blueprint of our study, and we present a preliminary evaluation. The numerical results illustrate that the scheme can improve data caching capability by 29.3% in the deployment of future wireless sensor networks.**

Keywords- Information-centric network (ICN); Wireless sensor network (WSN); Unmanned aerial vehicle (UAV); Cross-layer.

I. INTRODUCTION

Smart cities bring intelligence to various aspects of our daily lives for rapid urbanization, and there are application services to realize them, such as smart homes, personal healthcare, and urban infrastructure management. In addition, smart cities alternatively include not only urban sophistication, but also resilience to serious disasters and the promotion of public healthcare during global pandemics. Those promises have been recognized as representative of the Internet of Things (IoT), and they feature a diverse array of cyber-physical systems. In realistic cities, to facilitate decision making and task execution for us, a massive number of resources, such as sensors, actuators, and data storages, need to be deployed to retain the sustainability of extensive social applications. Therefore, the smart cities' platform should be considered in practical data management through all protocol layers. In our study, we concentrate on an effective sensing data collection and management scheme for Wireless Sensor Networks (WSNs) while taking into account the aforementioned background. In particular, we introduce two key technologies into our proposed scheme: an Information-Centric Network (ICN) design [1] and a technique for assisted data collection of Unmanned Aerial Vehicles (UAVs) [2], which we call the UAV-assisted Information-Centric WSNs (UAV-IC-WSNs).

In conventional IoT frameworks, Sensor Nodes (SNs) are directly linked to cloud servers to gather and centralize sensing data via HTTP/TCP/IP-enabled application programming interfaces. Typical location-dependent common interfaces are reasonable for coordinating across multiple systems in distributed wireless networks; nevertheless, heavy address-based queries cause serious protocol overhead, making them similar to denial-of-service attacks. The ICNs name content data instead of the "address," and the ICN nodes copy and store the named data as caching data for further responses. Another problem with the current systems is that practical SNs are non-uniformly scattered depending on the ground surface, cost-effectiveness, and need to supply. Therefore, the sensing data are periodically generated but must be collected at asynchronous intervals. For data collecting and forwarding in those occasions, UAVs, such as drones (including multi-copters), small planes, and balloons, can work more flexibly and robustly as mobile sink nodes, which play an essential role in air-ground integration networks.

In our previous study [3], we have found that the proposed scheme cannot be used in the typical fourth-generation (4G) and fifth-generation (5G) WSN scenarios. Especially, the proposed scheme cannot accommodate into the traditional WSN system because of a huge sensing data traffic due to massive SNs. Therefore, sophisticated channel access mechanisms and efficient radio bandwidth utilization techniques must be considered as the remained works. In addition, studies on UAV-IC-WSN's Medium Access Control (MAC) protocols and physical protocols have remaining research problems [4]. Among them, in particular, acceleration in the transmission requests of sensing data leads to serious conflicts, such as collisions and interferences. In our previous study [5], we investigated a kind of cooperative MAC protocol design to remove interference among SNs, which are categorized as a cooperative sensing data collecting framework [4]. For the above atmosphere, we believe that we can overcame those technical issues by cooperative transmission, collision avoidance, and interference cancellation.

The cooperative MAC protocols can be basically classified as being either receiver-side or transmitter-side cooperation schemes. The receiver-side cooperation scheme is suitable for wireless networks to maximize their network lifetime because the rich receiver-side station nodes undertake complicated cooperative procedures. In fact, the fifth generation and beyond wireless network systems utilize UAVs as airborne base stations, and the UAV swarms provide

 ISBN: 978-1-61208-837-2

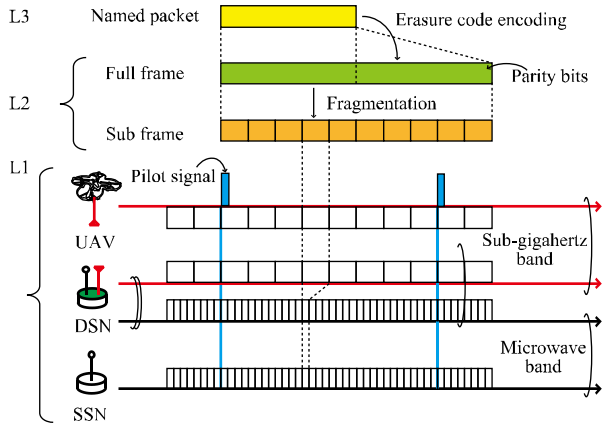


Figure 1. The relationship between the named packet and frame, the structure of the full-frame and sub-frame, and the relationship between the frame and time slot in two radio frequency bands

an integrated receiver-side cooperative reception mechanism [6]. However, we believe that cooperation at receivers is not sufficient to provide enormous sensing data transmissions. To tackle the aforementioned situation, we designed a novel joint sensing, forwarding, and storing scheme, which includes transmitter-side cooperation. To achieve the aforementioned mechanism, as the first steps, we introduce an erase code technique [7] and cross-layer optimization [8] into UAV-IC-WSNs. In this paper, we provide the overall blueprint of our study in progress, including a novel MAC and physical protocol design and a first fundamental evaluation of the scheme using a computer simulation. In particular, the key contribution of this paper is to solve the technical issues about channel capacity in UAV-IC-WSNs under 4G/5G scenarios by using dual-band SNs with erasure correction codes.

Related studies in UAV-IC-WSNs have investigated several elemental technologies. For example, Bithas et al. [9] investigated channel modeling to satisfy the requirements for massive connectivity and ultra-reliability. Li et al. [10] investigated the upper limitation of CSMA/CA-based MAC protocols and created an extended proposal. Bouhamed et al. [11] found the MAC protocols have flight path controls and trajectory optimization for UAV swarms, e.g., adaptation of machine learning techniques. As we could observe from the above literatures, there have been studied elementally wireless connectivity including antenna design and interference cancellation. Regarding an erase code technique, there have been typically studied in the field of distributed storage reliability [7]. For example, Kishani et al. [12] investigated the redundant array of independent disks. On the other hand, several studies have applied this technique in network research fields, e.g., Sharma et al. [13] utilized as an elemental technology to achieve the multipath diversity-based packet loss-tolerant network systems.

The remainder of this paper is organized as follows. Sectione II describes the proposed scheme. Section III presents the numerical results. Finally, Section IV summarizes our findings and concludes the paper.

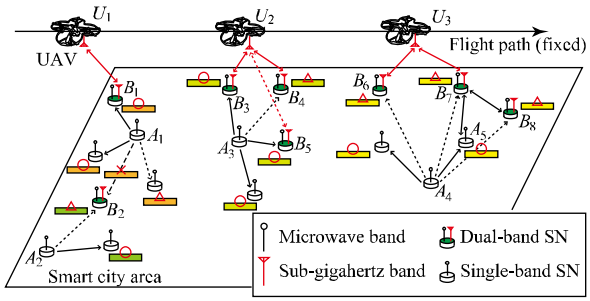


Figure 2. Network model

II. PROPOSED SCHEME

In the UAV-IC-WSN scheme, SNs are scattered on the ground in the smart city area, and the SNs observe and cache sensing data. Then, flying UAVs collect the data as necessary. In this section, we provide a network model, the MAC protocol, and the physical protocol.

A. System Description

As shown in Figure 1, the named packet for the packet/frame format is encoded based on the erase code, i.e., the full-frame is structured by appending the parity bits. We can select among Error Control Codes (ECCs) (that is utilized as forward error correction methods) with strong resistance to burst bit errors, such as the Low-Density Parity-Check (LDPC) code and the Reed-Solomon code. This is because the packets with any lost sub-frames have continuous bit errors in the sector of the lost sub-frames. Another motivation for introducing the erase code is that the original packet can be restored even if all the sub-frames are not complete. Therefore, retransmission procedures, such as automatic repeat request methods, are not necessary when the SNs intermittently execute so as to ensure low energy consumption. Furthermore, we can try to recover the packets by fetching the lost sub-frames from the neighbor SNs.

In the wireless air interface, our system utilizes and switches to two radio frequency bands: the microwave band and the sub-gigahertz band. Note that multiband wireless communication modules were adopted in several studies [14]. In general, higher frequency radio leads to larger data capacity and strong straightness (low diffraction). Therefore, our scheme assigns the microwave band radio and sub-gigahertz band radio for the wireless transmission areas between SNs and between a UAV and SN, respectively. We proposed the utilization of those spectrum bands because we suspect the familiar Low-Power Wide-Area (LPWA) networks, which typically use sub-gigahertz bands, will have difficulty wirelessly transmitting a large number of sensing data in future WSN scenarios, which are illustrated in the numerical results.

B. Proposed MAC protocol

The MAC protocol is designed based on the slotted-ALOHA scheme because we assume that all nodes can be synchronized using the pilot signal that the UAVs broadcast.

 ISBN: 978-1-61208-837-2

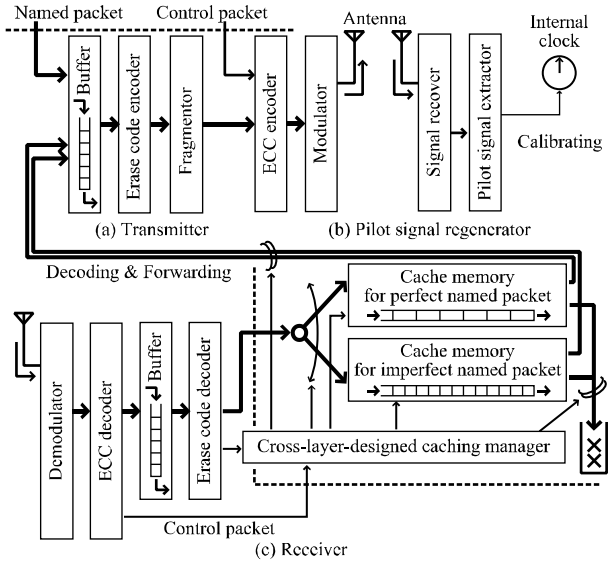


Figure 3. Procedure of wireless communication system

TABLE I. SIMULATION PARAMETERS

Terms	Values
Erase code	LDPC with sum-products decoding
Trans. Interval	600 s (= 10 min.)
Multiple access	Slotted-ALOHA
Number of channels	15
Full-frame length	64,800 bit
Number of fragmentations	60
Modulation method	BPSK
Error control coding	Convolutional coding
Radio Frequency	2.4 GHz (in microwave), 920 MHz (in sub-GHz)
Channel model	Rayleigh fading
Radio propagation model	Erceg's model (SN-BS), Amorim's model (SN-UAV)
Radio transmission power	0 dBm
Antenna gain	0 dBi
Circuit loss	0 dB
Thermal noise	−172 dBm

In general, the wireless communication system has a significant feature in that it is able to overhear what neighbor nodes can receive whether they desire it or not. In our system, to accelerate the effect of the caching processing, the nodes should actively accumulate the overheard data, making it the so-called off-path caching mechanism. For example, in Figure 2, $\mathbb{A}_1$'s data should be cached in not only $\mathbb{B}_1$ but also in neighbor SNs. However, if $\mathbb{A}_2$'s data are sent at the same time as $\mathbb{A}_2$'s, the data will interfere with each other. Regardless of the circumstances, $\mathbb{B}_2$ should be caching a part of $\mathbb{A}_2$'s data as the imperfect full-frame.

To select the dual-band SN to which the UAV gives a transmission request, first, the UAV broadcasts the interest packets to the area where the desired data might be located. If one node responds to the request, the UAV can decide on it, e.g., $\mathbb{U}_1$ selects $\mathbb{B}_1$. However, if there are several candidate SNs, the UAV can decide on the SN with the best wireless condition that is obtained using the signal strength of the responding packet among the dual-band SNs that have a perfect full-frame, e.g., $\mathbb{U}_2$ selects $\mathbb{B}_3$ among $\mathbb{B}_3$, $\mathbb{B}_4$, and $\mathbb{B}_5$. Moreover, if the candidate SNs have only imperfect data, the UAV tries to combine and restore the data, e.g., $\mathbb{U}_3$ selects and recovers both $\mathbb{B}_6$ and $\mathbb{B}_7$. Note that, we assume in this paper that the wireless connection between the UAV and the dual-band SNs is one hop because the current sub-gigahertz wireless systems are typically single hop with the end devices connected to a central gateway through a direct link. However, we believe that further packet loss can be improved if multiple hops are acceptable, and this is part of our future work.

C. Proposed physical protocol

The signal processing of the proposed wireless communications system is illustrated in Figure 3. As shown in Figure 3 (a), the full-frame is constructed at the erase code encoder by appending the parity bits that are calculated based on the named packet; and then, the full-frame is divided into several sub-frames at the fragmentor. Each sub-frame is encoded using the Error Control Code (ECC), such as the convolutional code, for error detection and correction through wireless links. After that, the codewords are mapped into the analog signals using the modulator, such as the binary phase shift keying method. To utilize the slotted-ALOHA scheme as the multiple access mechanism, we obtain the synchronization signals from the UAVs using the pilot signal regenerator, as shown in Figure 3 (b).

At the receiver side, as shown in Figure 3 (c), the received signal is demodulated and interpreted using a method such as Viterbi decoding. The correctly received sub-frames are stacked into a temporary buffer, and the erase code decoder tries to recover the original packet using sufficient sub-frames in the temporary buffer. As a result, if the restoring process is completed, the recovered packet is stacked in the cache memory for the perfectly named packet; otherwise, the failed packet is stacked in another cache memory for the imperfectly named packet. Therefore, the packets stored in those cache memories could be re-transmitted when the cooperative packet/frame transmissions are requested by other SNs and when the request is accepted. In addition, our proposed methodology requires collaboration beyond the boundaries among the lower three layers; thus, we believe that the caching manager must be created based on the cross-layer design.

III. NUMERICAL RESULTS

Our initial evaluation of the proposed scheme included the erase code technique's capability, the frame reachability through wireless channels, and the improvement in data caching among SNs. The simulation parameters are shown in Table I. We utilized the LDPC code as the erase code, and its parity-check matrix was decided based on the DVB-S2 specifications, which are widely utilized in digital video broadcasting via telecommunications [15]. The full-frame

length was decided based on the codeword length of the LDPC code, and the sub-frame length was decided based on typical LPWA systems. In this paper, to avoid system complexity, we assume that the buffer size is an ideal condition, i.e., we ignore the upper limitation of cache memory causing hardware devices, and we do not consider the selection of buffered sensing data. The radio propagation models utilized Erceg's model [16], Amorim's model [17], and the theoretical free-space model. Note that the first two models were done based on the practical measurement results, and the fading and shadowing were taken into account, unlike with the theoretical free-space model.

Regarding the robustness of the LDPC-based erase code, Figure 4 (a) shows the probability of successful recovery of the original packet if several sub-frames were lost. When the code rate R = 1/4, 1/3, 1/2, 2/3, and 3/4, the original packet could be reconstructed even if 4, 11, 7, 3, and 2 sub-frames were lost, respectively. Note that the code rate denotes the percentage of information data length in the total codeword length, including parity bits. In addition, the LDPC code has strong resilience to burst errors, but it requires a long codeword to guarantee sufficient error correction; therefore, we need to overcome this barrier for short sensing data message. In addition, in Figure 4 (a), when the percentage of lost subframes is small, the reason why the curve keeps a flat shape is enough subframes to recover a full-frame can arrive. On the other hand, the recovery rate suddenly degraded because the received data is digitally decoded; thus, there is no resistance to noise as same as an analog system.

The LDPC code decoder fulfills an iterative operation based on the belief propagation, which is called the sum-products algorithm. Figure 4 (b) shows the average number of iterations until a successful recovery, i.e., the computational burden increases depending on the increased number of iterations. As a result, the number of iterations was 10 times or less when the packet was successfully restored, and even if the number of iterative operations exceeded 50 times, no improvement occurred. In other words, in Figure 4 (b), the curve keeps flat shape when the number of iterations exceeds 50 times because the iterative decoding process reaches the pre-defined upper limitation. Note that, in Figure 4 (a) and (b), the radio propagation models are not taken into account because those simulations are performed based on lost subframes as parameters; thus, there is no effect of difference among radio propagation models. Figure 4 (c) shows the frame reception probability versus the distance between nodes. As a result, Erceg's model and Amorim's model describe smooth curves, and Amorim's model did not appear to be a difference between radio frequency bands.

Figure 4 (a)–(c) demonstrate the effectiveness of our scheme for packet caching, and Figure 4 (d) shows the computer simulation results. In general, 10,000/km^2 (in the 4G scenario), 1,000,000/km^2 (in the 5G scenario), and 10,000,000/km^2 (in the Beyond 5G (B5G) scenario) were assumed as the number of SN deployments. In Figure 4 (d), the LPWA systems achieved high reachability in the 4G scenario due to sufficient capacity for generated traffics. Therefore, the first computer simulation indicates that the proposed UAV-IC-WSNs can work under the 5G scenario by

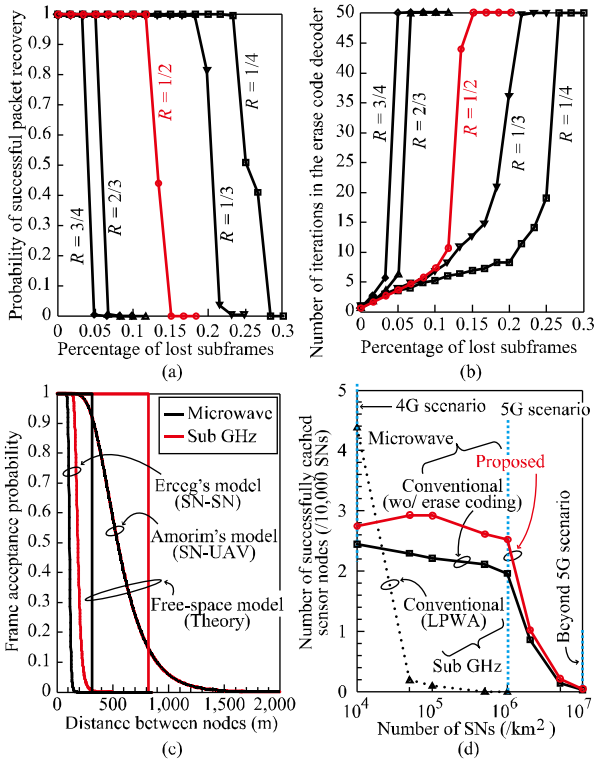


Figure 4. Simulation results: a) probability of successful packet recovery versus percentage of lost subframes, b) number of iterations in the erase code decoder versus percentage of lost subframes, c) frame acceptance probability versus distance between nodes, and d) number of successfully cached SNs versus density of distributed SNs

using the proposed MAC and physical protocols, while the traditional IoT frame cannot work in our previous studies. In particular, the proposed scheme improved data caching capability by 29.3% in comparison with a comparable scheme without introducing an erase code mechanism. The preliminary evaluation led us to conclude that our scheme has significant limitations for the B5G scenarios and needs further analysis.

IV. CONCLUSION

This paper proposed a novel erase code-enabled data caching scheme for UAV-IC-WSNs to achieve joint sensing, forwarding, and storing. We provided the overall blueprint of our proposal and a fundamental evaluation. As future work, we will expand on the B5G scenarios and analyze them in practical environments. In addition, it is necessary to discuss the disadvantages of dual-band SNs compared to single-band SNs in terms of power consumption and implementation cost.

ACKNOWLEDGMENT

A part of this work was supported by JSPS KAKENHI Grant Number JP19K20261.

REFERENCES

[1] S. Arshad, M. A. Azam, M. H. Rehmani, and J. Loo, "Recent Advances in Information-Centric Networking-Based Internet

of Things (ICN-IoT)," *IEEE Internet of Things Journal*, vol. 6, no. 2, pp. 2128–2158, Apr. 2019.

[2] F. Qi, X. Zhu, G. Mang, M. Kadoch, and W. Li, "UAV Network and IoT in the Sky for Future Smart Cities," *IEEE Network*, vol. 33, no. 2, pp. 96–101, Mar. 2019.

[3] S Mori, "A Fundamental Analysis of Caching Data Protection Scheme using Light-weight Blockchain and Hashchain for Information-centric WSNs," *Proc. 2nd Conf. Blockchain Research & Applications for Innovative Networks and Services (BRAINS 2020)*, Sept. 2020, pp. 200–201, doi: 10.1109/BRAINS49436.2020.9223279.

[4] S. Poudel and S. Moh, "Medium Access Control Protocols for Unmanned Aerial Vehicle-Aided Wireless Sensor Networks: A Survey," *IEEE Access*, vol. 7, pp. 65728–65744, 2019.

[5] S. Mori, "Cooperative Sensing Data Collecting Framework by using Unmanned Aircraft Vehicle in Wireless Sensor Network," *Proc. IEEE Int. Conf. Commun. (ICC2016)*, May 2016, pp. 1–6, doi: 10.1109/ICC.2016.7511187.

[6] S. Zhang, H. Zhang, and L. Song, "Beyond D2D: Full Dimension UAV-to-Everything Communications in 6G," *IEEE Trans. Vehicular Tech.*, vol. 69, no. 6, pp. 6592–6602, June 2020.

[7] K. V. Rashmi, N. B. Shah, K. Ramchandran, and P. V. Kumar, "Information-Theoretically Secure Erasure Codes for Distributed Storage," *IEEE Trans. Info. Theory*, vol. 64, no. 3, pp. 1621–1646, Mar. 2018.

[8] V. Srivastava and M. Motani, "Cross-layer Design: A Survey and the Road Ahead," *IEEE Commun. Mag.*, vol. 43, no. 12, pp. 112–119, Dec. 2005.

[9] P. S. Bithas, V. Nikolaidis, A. G. Kanatas, and G. K. Karagiannidis, "UAV-to-Ground Communications: Channel Modeling and UAV Selection," *IEEE Trans. Commun.*, vol. 68, no. 8, pp. 5135–5144, Aug. 2020.

[10] B. Li, X. Guo, R. Zhang, X. Du, and M. Guizani, "Performance Analysis and Optimization for the MAC Protocol in UAV-Based IoT Network," *IEEE Trans. Vehicular Tech.*, vol. 69, no. 8, pp. 8925–8937, Aug. 2020.

[11] O. Bouhamed, H. Ghazzai, H. Besbes, and Y. Massoud, "A UAV-Assisted Data Collection for Wireless Sensor Networks: Autonomous Navigation and Scheduling," *IEEE Access*, vol. 8, pp. 110446–110460, 2020.

[12] M. Kishani, S. Ahmadian, and H. Asadi, "A Modeling Framework for Reliability of Erasure Codes in SSD Arrays," *IEEE Trans. Computers*, vol. 69, no. 5, pp. 649–665, May 2020.

[13] V. Sharma, S. Kalyanaraman, K. Kar, K. K. Ramakrishnan, and V. Subramanian, "MPLOT: A Transport Protocol Exploiting Multipath Diversity Using Erasure Codes," *Proc. Int. Conf. Computer Commun. (INFOCOM2008)*, Apr. 2008, pp. 121–125, doi: 10.1109/INFOCOM.2008.33.

[14] Z. M. Fadlullah et al., "Multi-Hop Wireless Transmission in Multi-Band WLAN Systems: Proposal and Future Perspective," *IEEE Wireless Commun.*, vol. 26, no. 1, pp. 108–113, Feb. 2019.

[15] DVB project: https://dvb.org [retrieved: Jan. 2021].

[16] V. Erceg et al., "An Empirically Based Path Loss Model for Wireless Channels in Suburban Environment," *IEEE J. Sel. Areas in Commun.*, vol. 17, no. 7, pp. 1205–1211, July 1999.

[17] R. Amorim et al., "Radio Channel Modeling for UAV Communication Over Cellular Networks," *IEEE Wireless Commun. Lett.*, vol. 6, no. 4, pp. 514–517, Aug. 2017.

 ISBN: 978-1-61208-837-2

Security Vulnerabilities of Popular Smart Home Appliances

Fida Hussain, Abhaya Induruwa (Retired), Man Qi
School of Engineering, Technology and Design
Canterbury Christ Church University
Canterbury, United Kingdom
e-mail: fh51@canterbury.ac.uk; beko539@gmail.com; man.qi@canterbury.ac.uk

***Abstract*—A Smart Home (SH) essentially is a communication network that connects smart devices, sensors and actuators, enabling the owner to locally and remotely access, monitor and control them. However, SHs are currently facing increasing challenges due to the underlying home automation systems, which are affected by network security issues. This paper presents an SH testbed comprising SH devices that employ IEEE 802.11 standard protocol for communication. Comprehensive tests were conducted using the testbed that incorporated popular SH devices with the aim to observe and understand vulnerabilities that exist in smart device networks when they are attacked using different types of attacks, such as Eavesdropping, Denial of Service (DoS), and Man-In-The-Middle (MITM). This paper presents the details of the SH testbed and reports and discusses the findings obtained from these experiments.**

Keywords-Smart Homes; device vulnerabilities; Smart Home Testbed; Eavesdropping; DoS; MITM attacks.

I. INTRODUCTION

SH is a user-oriented home communication system where gadgets are interconnected through a local network and exposed to the Internet, so that it can be remotely controlled from anywhere through the Internet by using network or mobile devices (smartphone or tablet). Gadgets on a SH network permit the authentication of a user to control different tasks, such as temperature control, adjusting the lighting, locking-unlocking of doors, and security access to the home from a distance [1]. Different apps can be installed on a smartphone or other devices connected to the network, or the user can use a timer programme and set up a schedule.

Some smart home appliances come with artificial intelligence (self-learning skill) so they can learn homeowner behaviour over time and alert the user or react by making necessary changes when something out of the ordinary happens [2][3]. They will alert the user if they detect suspicious activities for example, when motion is detected in the home when the user is away. Smart Homes face different challenges due to issues and features related to home automation systems. These include home automation standards, high installation costs, varying consumer inexperience with technology, additional and support costs, limited cooperation of smart devices manufacturers, complex user interfaces and security challenges from different security threats [2].

Connecting the SH to the Internet gives the user almost 24x7 access to it, subject to the availability of Internet. This allows the attacker from either locally, or remotely anywhere in the world to target the SH [4]. Such an attacker can scan for certain vulnerabilities related to a specific device or can keep searching until a particular vulnerability they are looking to exploit is found.

Internet of Things (IoT) devices that are used in SHs use different Wireless Local Area Network (WLAN) protocols, such as Bluetooth, ZigBee, Z-Wave, and IEEE 802.11. Due to convenience, most smart devices in SHs use IEEE 802.11variants. The legacy IEEE 802.11, released in 1997 and clarified in 1999, is now obsolete but the newer variants based largely on Orthogonal Frequency Division Multiplexing (OFDM) have witnessed continuous growth in popularity [5]. In current times, WLAN 802.11n through to 802.11ah are the more popular and successful indoor wireless solutions, having progressed as a key enabling technology to cover smaller to large organisations, public area hot-spots and so on [6]. The IEEE 802.11 standardisation committee has actively pursued to publish new draft modifications to integrate with up-to-date technologies and current challenges. However, there are currently different security challenges facing IEEE 802.11 based WLANs, such as Eavesdropping, DoS, MITM attacks, and so on.

For the purpose of the study reported in this paper, the SH testbed has been created by using different SH devices, which use the IEEE 802.11 standard protocol to communicate. To find vulnerabilities present in these devices forming the SH network, different types of attacks have been performed. The rest of this report is organised as follows.

Section II is a literature review. Section III is a summary of different types of attacks and their importance to a SH application. Section IV describes the smart devices used in developing the SH testbed. Section V presents the results that were achieved by performing different experiments (different attacks) using the SH testbed. Finally, Section VI closes the paper with conclusions and some ideas for future work.

II. REVIEW OF RELATED WORK

Alsahlany, Almusawy and Alfatlawy [7] analysing the risk of a fake Access Point (AP) attack against Wi-Fi networks, discuss the security issues of the Wi-Fi user, such as those posed by fake APs. They have carried out experiments by creating fake APs to launch a MITM attack to sniff, capture and analyse the victim's traffic. However, their scope is somewhat limited as the work focuses only on a fake AP attack against Wi-Fi networks, but the chances that the user would connect to the fake AP are rather low.

Jose and Malekian [4] explain the different SH structures from a security viewpoint. They examine the current security flaws and challenges in home automation systems from the standpoint of both the homeowner and the security engineer. They have carried out a literature review about the challenges faced by home automation, but have not set up an SH testbed

 ISBN: 978-1-61208-837-2

to carry out experiments to find vulnerabilities and apply suggested security measures.

Kilincer, Ertam and Şengür [8] propose an automated technique to detect and prevent fake AP attacks in a network with IoT devices. In the experiment, they use a Single Board Computer (SBC) and a wireless antenna (ODROID module). The whole operation has been divided into three stages. In the first stage, a fake AP broadcast has been created. The second stage is to scan the surroundings using the SBC and Wi-Fi modules and in the last stage, to prevent detecting fake AP broadcasts. The fake AP has been assigned to an unauthorised Virtual Local Area Network (VLAN). This research is limited and focuses on fake AP attack detection and prevention, but the data collection about the network and some of the attacks are still possible without connecting to it.

Doughty, Israr and Adeel, [9] have studied vulnerabilities in six different Internet Protocol (IP) cameras by performing various attacks using Address Resolution Protocol (ARP) poisoning. Their findings show that IP cameras are still vulnerable to ARP poisoning and spoofing, and the criminals can take advantage of it. Due to the lack of security in devices and applications, they remain insecure to ARP poisoning. At the end of their research, they suggest methods of preventing ARP poisoning. Their research is limited to some IP cameras, and not to other SH devices where ARP poisoning attack is possible when used as part of an SH network.

Yoon, Park and Yoo [10] analyse security vulnerabilities in SHs in IoT environments and propose countermeasures. Although they talk about different vulnerabilities and countermeasure, such as trespass, monitoring and personal information leakage, DoS/ Distributed Denial of Service (DDoS) attacks and falsification, all of which are possible to happen in SHs, they have not set up an SH testbed to carry out experiments to find the sugested vulnerabilities and study how to prevent them with counter measures.

Davis, Mason and Anwar [11] conducted vulnerabilities and security posture studies of smart home IoT devices. They conducted their own vulnerabalities experiments that compared security posture between well known and less known vendors through misuse and abuse case analysis. Based on their analysis, the main finding was the need for a stronger focus on the security posture of lesser known vendor devices. Their approach utilised software engineering modeling methods, such as use cases, misuse cases, and abuse cases. These use cases were defined based on the device functionality and assumptions of interconnectivity by the manufacturer. However an SH testbed was not setup to carry out these experiments.

III. NETWORK SECURITY THREATS FOR IOT IN THE SH

Based on their key features, wireless protocols can be further divided into different communication protocols, such as ZigBee, Wireless Fidelity (Wi-Fi), Z-Wave, IPv6 Low-power wireless Personal Area Network (6LoWPAN), Bluetooth, etc. [12]. The properties and key features of these protocols are shown in Table I. Due to high bandwidth and fast speed, wireless is most used everywhere [13], and most IoT devices use a wireless connectivity protocol. The work reported in this paper is based on IoT devices that use Wi-Fi connectivity (IEEE 802.11x). Due to the high use of IEEE 802.11x by different devices nearly everywhere, including IoT in houses, hospitals, and hotels, they attract a lot of attention of attackers to launch different types of attacks either remotely or locally for different motives. Some of the common types of local attacks that are still dangerous to local IoT devices are eavesdropping (aka sniffing or spoofing), de-authentication, and man-in-the-middle, which are further explained in the next sections.

TABLE I. WIRELESS PROTOCOLS AND THEIR FEATURES

Features	Wireless Protocols				
	Wi-Fi	**ZigBee**	**Z-Wave**	**Bluetooth**	**6LoWPAN**
Standardisation	IEEE 802.11a/ b/g	IEEE 802.15.4	Proprietary	IEEE 802.15.1	IETF
Frequency band	2.4GHz, 5GHz	868/915 MHz, 2.4GHz	900MHz	2.4GHz	868MHz, 900MHz and 2.4GHz
Range (m)	46/ 92	10-100	30	1, 10, 100	20
Security algorithm	WPA, WPA2	AES-128	AES-128	E0, E1, E3, E21, E22 56-128 bit	AES- 128
Topology	one-hop	star, tree, mesh	star, mesh	p2p, scatternet	mesh
Channel bandwidth	22MHz	0.3/0.6 MHz, 2MHz	300kHz, 400kHz	1MHz	600kHz, 2MHz, 5MHz

A. Eavesdropping Attack

This is also known as sniffing or spoofing attack. It is used to sniff the network traffic in wireless networks that connect IoT devices via Bluetooth, IEEE 802.11x, or Radio Frequency Identification (RFID). It is carried out by illegally impersonating a legal IoT device to gather information via sniffing [14]. Eavesdropping attack is an important first step before launching any type of attack on IoT devices. For example, by the launch of this attack an attacker can obtain passwords, credit card numbers, emails, documents, browsing history, login details, File Transfer Protocol (FTP) login details, FTP documents, web addresses, and other confidential information, that users or devices may normally send over the network [15].

This kind of attack is performed to gain illegal access to information to launch de-authentication or man-in-the-middle attack [16]. It gathers all types of traffic including encrypted traffic. A tool, such as Sniffer may be used to sniff packets to gather information. It is impossible to detect and penetrate vulnerabilities on the system's (i.e., computer's) wireless adapter. Therefore, to manage and monitor IEEE802.11 b/g/n devices' traffic, two types of wireless adapters, namely ALFA AWUS036NHA 2.4 GHz and ALFA AWUS036ACH 2.4 & 5 GHz were used. These wireless adapters have been used as they are compatible with IEEE802.11 b/g/n traffic, and work with a maximum connection rate of 150 Mbps [7]. When devices are communicating with each other using wireless protocols, their Medium Access Control (MAC) addresses are encrypted.

 ISBN: 978-1-61208-837-2

It is known in packet communications basics that a MAC address makes sure that a packet is delivered only to the right destination (identified by the recipient's MAC Address). This in turn leads to the question how a device can receive a packet which is not destined for it? In sniffing, since Wi-Fi packets are present all around in an area within a specific range, i.e., the wireless footprint, the external wireless adapter is used by the attacker after changing the setup from 'manage mode' to 'monitor mode'. Doing this makes it possible to capture all the packets in the surrounding Wi-Fi range.

To change a wireless adapter from manage mode to monitor mode, an open-source tool called Airodump-ng, which also includes an Aircrack-ng package, has been used. Aircrack-ng is a tool used for analysing network security, especially by monitoring, attacking, testing and cracking Wi-Fi networks [7][17][18].

Once the attacker selects a specific network to target, the attack is launched by giving a specific AP MAC address, a channel with monitor mode to write (save) the data in a file so it can be analysed later. By analysing the saved file some useful information, such as manufacturer's name and MAC address of all devices that are connected to that specific AP, can be found. A de-authentication attack can be launched by a tool called Aireplay-ng [7], which enables the attacker to disconnect specific devices by using their MAC addresses.

B. Denial of Service (DoS) De-authentication attacks on 802.11 based networks

DoS is a challenging attack on computing devices, caused by bombarding with requests during a certain period, forcing the target devices to crash, go-slow, or shutdown altogether [19]. As IoT devices are limited in resources, DoS attacks may cause more damage to them [20]. Most IoT devices use low priced hardware with low-cost deployment of IEEE 802.11-based networks. Due to their popularity, IoT devices (roughly 30 billion devices in use in 2020) and 802.11 networks are attacked by the largest number of attackers [20][21]. Researchers are working hard to fix these vulnerabilities in 802.11 networks by bringing out different security standards in the protocol, such as Wi-Fi Protected Access (WPA), Extensible Authentication Protocol (EAP), 802.11i, 802.1x [22]. Even so, there are still some vulnerabilities that are not yet dealt with by any of these security standards. One such attack is the de-authentication attack. 802.11 networks can operate in infrastructure mode (i.e., devices communicating with one another by first going through an access point) or in ad-hoc (peer to peer) mode. An 802.11 network, when operating in infrastructure mode, needs the wireless device to connect to an AP before the data messaging takes place. In this process the device needs to validate itself to the AP before communicating with the AP. If either the client device or the AP wants to disconnect itself from the other, they send a de-authentication frame to leave the network. When client devices and AP are communicating with each other these frames are unencrypted, and an attacker can easily spoof these frames, which have the unencrypted MAC addresses of the devices and the AP. Using them, the attackers can easily launch a DoS attack (de-authentication attack) to disassociate the client device from the AP.

In a pre-connection type of attack, where the attacker is not part of the network, a DoS attack that targets communication between the AP and the gadget is launched allowing the attacker to disconnect the gadget from the network for a certain period of time defined by the attacker. The attacker sends a packet to the AP and the target device, therefore it will disconnect the device for a defined period of time. This kind of attack can be used to disable SH IoT devices, such as a Closed Circuit Television (CCTV) IP camera, gateway, smartphone, or any other device present in home automation to gain access to the home without notice [23]. In this, the attacker sends packets to the router by pretending that it is a target device using the spoofed MAC address. In the meantime, the attacker is pretending to be a router to the target and is telling it to re-authenticate itself. This is a kind of ethical hacking attack performed by placing different gadgets like Amazon Echo, Google Home, Android smartphone, iOS phone, Android tablet and IP Dynamode Camera.

This kind of attack is useful to the attacker in many ways. It is very useful in social engineering exercises where you could disconnect clients from the target network, and then call the user and pretend to be a person from the IT Department and trick them to install a virus or a backdoor. The attacker can also create another fake access point and persuade the gadgets to connect to the fake access point to spy on them, sniff and spoof their traffic. Besides, it is also possible to launch a man- in-the-middle attack because the attacker would have gathered all the useful information. This kind of attack can also be used to capture the handshake, which is vital when it comes to WPA cracking.

C. MITM (Man-In-The-Middle) attack

It is the type of attack where the attacker successfully changes the communication between two parties (i.e., sender and receiver), where the sender and receiver believe that they are communicating with a genuine party but the entire communication is controlled by the attacker. MITM can be known by different names like Bucket-brigade attack, Fire brigade attack, Monkey-in-the-middle attack, Session hijacking or Transmission Control Protocol (TCP) hijacking. Before the MITM attack is lunched, the communication traffic is only monitored and read. This is a passive act, but it gathers plenty of information to launch the subsequent attacks.

An MITM attack can be implemented through different ways, but in the testbed, it has been implemented by 1) using fake access point, and 2) by using ARP poisoning. A fake access point can be set up by using the information, such as MAC address, channel, and Service Set Identifier (SSID), that was gathered by sniffing and spoofing. Using a tool called Mana-toolkit in Kali Linux, a fake AP will be configured to have the same setup as the target AP, such as identical user name AP, but it will be a network without encryption and that broadcasts a strong signal by using a Network Interface Card (NIC), [1] such as ALFA AWUS036ACH, with an external antenna. Before connecting target devices to the fake AP, a DoS (de-

 ISBN: 978-1-61208-837-2

authentication) attack is launched to disable devices on the target network. When the target devices connect to the fake AP then the whole traffic will be going to the man-in-the-middle and it will make it easier to steal the information from the compromised devices. Method 2, ARP poisoning, is an attack performed on a LAN, where the attacker falsely advertises the MAC addresses of the default gateway and the target device and fools both devices to connect to the attacker. The ARP poisoning is only possible when the attacker is part of the target network. ARP poisoning can be carried out using a tool called Man-In-The-Middle framework (MITMf). MITMf is a powerful tool that can be used to intercept and modify the flow of packets between the victim and AP because the flow of the packet is now through the attacker. As all the traffic is going through the MITM, the attacker knows about the victim using the Internet.

IV. DEVELOPING THE SMART HOME TESTBED

To practically test, analyse and understand the security of SHs, an expert needs to develop an SH testbed containing a mix of different, random, IoT devices that are commonly found in a modern smart home. For this purpose, the testbed shown in Figure 1 has been developed by incorporating a range of devices representing home gateways, IP cameras, various smart phones and tablets, programmable single board computer, all connecting to the home router. The particular devices chosen are Amazon Echo, Amazon Dot, Google Home, smart IP Camera (IP Dynamode White DYN-630), IPhone4, Sony Xperia Tablet, and Nest Cam Indoor Security Camera. Amazon Echo, Amazon Dot, and Google Home are home gateways that allow voice control. They are all very popular and millions of people use them in their homes in everyday life to ease their life [24]. Amazon Echo and Google Home are smart speakers with the 'assistant features', using which the user can ask about the weather, news, use them as a search engine, in addition to controlling other smart devices that are connected to them. IP Dynamode White (DYN-630) is a wireless camera that has a range up to 8 metres. Among its features are zoom, motion detection, video support control, two-way voice talkback, and an external alarm which sends information directly to the server via email or FTP. With all these functionalities and an affordable price, it makes it perfect to use in a SH. Google Nest Cam Indoor Security Camera with a good quality picture (1080p), viewing angle with 130 diagonal degrees, private and secure communication (128-bit AES encryption, TLS, 2048-bit RSA private keys, Perfect Forward Secrecy) is more advanced than IP Dynamode. However, it is more expensive than IP Dynamode White (DYN-630). Sony Xperia Tablet Z LTE and Samsung Galaxy s7 edge are used as a user interface to install different SH apps to control and monitor systems. The Raspberry Pi 3 used in the SH testbed is a low cost, yet powerful, programmable computer. Among its many useful features is the General Purpose Input Output (GPIO) interface that is being used to create IoT solutions for the smart home. The testbed also includes an iPhone4. Although quite a few years old now, this is a smart device that is increasingly being used as DIY security cameras in SHs [25][26]. The use of old iOS

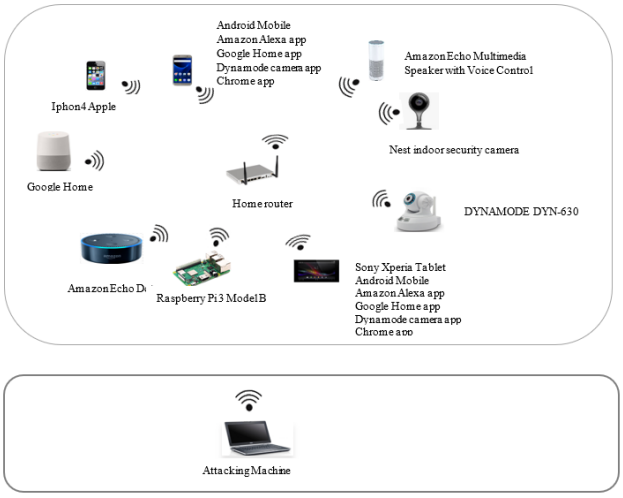


Figure 1. Smart Home Testbed

devices in SHs is an attractive proposition, but such appliances open up vulnerabilities and introduces security threats in SHs making it very important to understand how SH security landscapes are impacted with such use. It is in this context an old, but popular device, such as iPhone4 is included in the testbed.

After developing this testbed, different security tests were carried out. As it is impossible to detect and penetrate vulnerabilities on the system through a local wireless adapter in a laptop, two types of wireless adapters namely ALFA AWUS036NHA 2.4 GHz and ALFA AWUS036ACH 2.4 & 5 GHz were used to manage and monitor the devices' Wi-Fi traffic. Kali Linux is operating on the attacking machine. In the eavesdropping, de-authentication and fake Access Point attacks, it is playing the role of the outside attacker and in the ARP poisoning attack, it plays the role of an internal actor.

V. RESULTS

To get the results of these attacks, the attacker needs to go into monitor mode, which is called sniffing or spoofing (passive attack) where it sniffs all the traffic without a connection to an AP or to ad-hoc network. Collecting information in this stage is important in order to launch a further attack on the target device. All the APs and connected devices can easily be identified in a limited range. Figure 2 shows the features of the APs and devices that are connected to these APs after executing the Airodump-ng tool in the neighbouring area, and it provides us with very useful

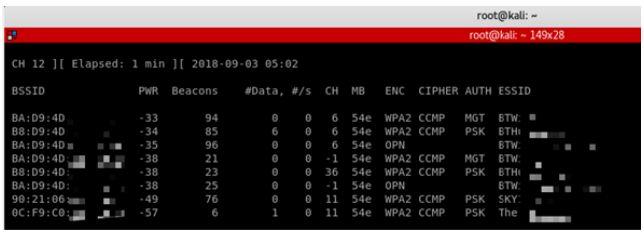


Figure 2. Features of the Access Points

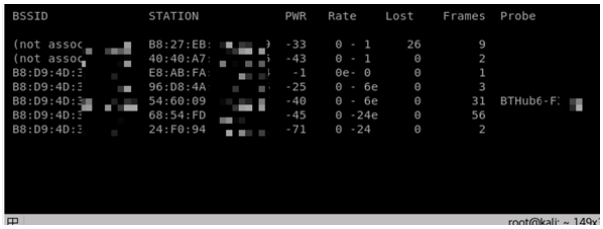


Figure 3. MAC addresses of the connected devices

information. The first column shows the Basic Service Set IDentifier (BSSID) also called the MAC address of all APs in the surrounding area. The AP signal strength (PWR) is shown in the second column in decibels (db). The highest db value means the AP is nearest to the attacker. Information about the channel of the AP is important where the CH column exposes the information about the AP in the channel they operate. Most APs are using encryption keys for connection but some of them are open and do not have an encryption key. ENC column shows whether encryption is being used. OPN indicates an open connection. The last column shows the Extended Service Set Identification (ESSID), the names of APs that are broadcasting.

The detailed information that has been obtained and shown in Figure 2 can be used to launch a de-authentication attack (DoS) on each individual IoT that is connected to the specific AP. To launch a de-authentication attack, the MAC addresses of the target AP and the IoT device connected to it are required. To obtain the MAC addresses of the connected devices to AP, Airodump-ng with MAC address of AP is needed to be launched.

Figure 3 shows the MAC address of the connected device to the target AP. It is easy to launch a de-authentication attack after obtaining the required information (MAC Addresses of AP and target device). Figure 4 shows the successful launch of de-authentication for a certain defined time period where the target device is not aware of it. The target will not be able to connect to the AP unless it is restarted, or the end period defined by the attacker has been reached. As shown in Table II, the voice control of Amazon Echo, Google Home, and

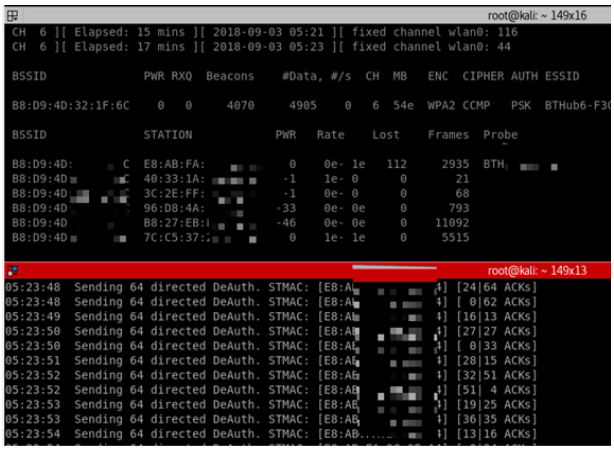


Figure 4. Launch of successful de-authentication attack

Amazon Echo Dot has strong resistance to a de-authentication attack. Although a de-authentication attack was successfully

TABLE II. RESULTS OF DE-AUTHENTICARTION ATTACK

IoT Appliances	De-authentication Attack
Amazon Echo Google Home Amazon Echo Dot	Connection interrupted. Unable to disable their connection from the AP.
Android Mobile (Model no. SM-G935F, SM-G930F) Nest Cam Indoor Security Camera	Sometimes connection interrupted and device disabled from the connected AP.
DYNAMODE DYN-630 Iphon4 Apple Raspberry Pi 3 Sony Xperia Tablet	Connection interrupted and device disabled from the connected AP

launched on the target devices the attacker was unable to disable the target devices' connections from the target AP.

However de-authentication was successful and Android mobile devices (Model nos. SM-G935F, SM G930F) were disabled when they were at roughly 10 metres from the connected AP. Furthermore, Nest Cam Indoor Security Camera was disabled for short duration of time (1 to 2 seconds) by the launching of de-authentication. As shown in Table II, IP DYNAMODE DYN-630, Apple IPhone4, Raspberry Pi 3 with Linux operating system, and Sony Xperia Tablet devices were successfully targeted, the connection was interrupted and the connection from the AP was disabled. This scenario presented the worst security concerns as they allowed every single attempt to drop their connection from any distance within the SH.

There are different ways to implement MITM attacks, but in the testbed, it has been implemented by using 1) fake access point and 2) ARP poisoning. In this experiment, as shown in Figure 5, the fake AP created is called Smart Home. It is similar to the target AP, but the fake Smart Home AP is without encryption. In this kind of situation, the attacker uses

Figure 5. Victim connected to fake AP

DoS attack to force devices to disconnect from the genuine AP and connect to the fake AP.

In this experiment, an attacker can force the smart devices by using de-authentication attack and target device connect to fake AP as shown in Figure 5. But as it was evident from previous tests, it is hardly possible to disable many devices from the legitimate AP. Also, it would be harder to convince the victim to use the fake AP. For these reasons, it is not highly successful to target the SH by using a fake AP.

ARP poisoning MITM attack is possible when an attacker is part of the network. To launch ARP poisoning in Kali Linux, MITMf tool was used to perform ARP poisoning but before using MITMf, the attacker has to scan the whole network using a scanning tool, such as NMAP to know the MAC address of the target device and the IP address of the default gateway (AP). The target device responds and sends its MAC address. The ARP table, the IP address and MAC address of different devices including the gateway becomes available to the attacker. The attacker knows in detail about the time and what website the victim is using. To further capture and analyse the data packets, the attacker can use Wireshark [7]. This way some other vulnerabilities, such as session hijacking and denial of services can be exploited.

VI. Conclusions and Future Work

The use of wireless Wi-Fi devices is growing day by day with the extensive use of the Internet. If adequate security measures are not taken, it could have serious implications for SH devices. There is the possibility to view, capture and modify the data packets by the attacker using the existing vulnerabilities in SH devices and IEEE802.11 b/g/n traffic captured by nefarious means. The primary contribution of the research work is building and evaluating a testbed suitable for finding security vulnerabilities and threats in SH networks incorporating both new and old IoT devices. The testbed can then be expanded to include many more diverse SH IoT devices as they become available, and explore their vulnerabilities and possible security attacks on them.

This paper demonstrates that due to vulnerabilities remaining in some SH devices they are prone to attacks, such as eavesdropping, DoS and MITM. Throughout the whole experiment, Kali Linux operating system was used with ALFA AWUS036NHA 2.4 GHz and ALFA AWUS036ACH 2.4 & 5 GHz wireless adapters. Eavesdropping attack was used to sniff the network traffic of the wireless network. An open-source tool called Airodump-ng was used to sniff packets to gather information that would allow to mount an attack. The tool gathers some useful information, such as MAC address, channel, and ESSID. This information can later be used to mount DoS and MITM attacks. This kind of attack could be fatal as the IoT device can be disabled for a certain period. For the MITM attack the Mana-toolkit and MITMf were used. The two MITM attack types, i.e., using fake AP and ARP poisoning have been used to target SH devices as they are more effective and can damage SH devices. To avoid de-authentication attack, the device need to have a wired connection to the network, or if the connection is wireless, use the IEEE 802.11w, the amendment adding management frame protection functionality to 802.11 standard. This amendment was brought to provide better protection to control and management frames against forgery, replay and disconnect attacks. Security can also be enhanced by enabling 802.11w/WPA3 combination. Although a fully-fledged discussion on WPA3 is beyond the scope of this paper, it is worth noting that WPA3 secures a device even when weak passwords are used or when an attacker attempts to crack them using brute force techniques. The AP can add Message Integrity Check Information Element (MIC IE) to each management frame it transmits to protect them against any attempt to copy, alter, or replay by invalidating the MIC. To protect broadcast/multicast management frames a new key called Integrity Group Temporal Key (IGTK) is used.

ARP poisoning can be detected through different ways, such as using an open-source packet analyser, e.g., Wireshark, or using proprietary options, such as XArp and command prompt. The easy way to finding an ARP poisoning attack is by opening a command prompt as administrator. Running command ‘arp –a’ will show ARP table IP address and MAC address of connected devices. In this table, if two different IP addresses are displayed with the same MAC address, then it is possible that the network undergoing an ARP poising attack. To prevent this kind of attack, the ARP table needs to be configured with the static IP address and the MAC address. Chances of connecting to fake AP may be low but the SH user needs to be educated to avoid connecting to fake APs and to use a Virtual Private Network (VPN) connection which will encrypt communication between sender and receiver. The testbed will be used to study and understand how future SH devices can be secured from these attacks, and hope to share the knowledge thus created with the community.

References

[1] J. Chen, "*Investopedia*," 2015. [Online]. Available from: https://www.investopedia.com/terms/s/smart-home.asp. [retrieved: February, 2021]

[2] V. S. Gunge and P. S. Yalagi, "Smart Home Automation: A Literature Review," International Journal of Computer Applications, pp. 6-10, 2016.

[3] K. E. Skouby and P. Lynggaard, "Smart Home and Smart City Solutions enabled by 5G, IoT, AAI and CoT Services," 2014 International Conference on Contemporary Computing and Informatics (IC3I), pp. 874-878, 2014.

[4] A. C. Jose and R. Malekian, "Smart Home Automation Security: A Literature Review," Smart Computing Review, vol. 5, no. 4, pp. 269-285, 2015.

[5] E. Perahia, "IEEE 802.11n Development: History, Process, and Technology," IEEE Communications Magazine, vol. 46, no. 7, pp. 48-55, 2008.

[6] M. S. Afaqui, E. Garcia-Villegas and E. Lopez-Aguilera, "IEEE 802.11ax: Challenges and Requirements for future High Efficiency WiFi," IEEE Wireless Communications, vol. 24, no. 3, pp. 130-137, 2017.

 ISBN: 978-1-61208-837-2

[7] A. M. Alsahlany, A. R. Almusawy and Z. H. Alfatlawy, "Risk Analysis of a Fake Access Point Attack Against Wi-Fi Network," International Journal of Scientific & Engineering Research, vol. 9, pp. 322-326, 2018.

[8] F. Kilincer, F. Ertam and A. Şengür, "Automated Fake Access Point Attack Detection and Prevention System with IoT Devices," Balkan Journal of Electrical & Computer Engineering, vol. 8, no. 1, 2020.

[9] T. Doughty, N. Israr and U. Adeel, "Vulnerability Analysis of IP Cameras using ARP Poisoning," 8th International Conference on Soft Computing, Artificial Intelligence and Applications (SAI 2019), June, 2019.

[10] S. Yoon, H. Park and H. S. Yoo, "Security Issues on Smarthome in IoT Environment," *SpringerLink*, vol. 330, pp. 691-696, 2015.

[11] B. D. Davis, J. C. Mason and M. Anwar, "Vulnerability Studies and Security Postures of IoT Devices: A Smart Home Case Study," *IEEE Internet of Things Journal*, vol. 7, no. 10, pp. 10102-10110, 2020.

[12] A. N. Gollu and J. Kumar, "Wireless Protocols: Wi-Fi SON, Bluetooth, ZigBee, Z-Wave, and Wi-Fi," in *Innovations in Electronics and Communication Engineering: Proceedings of the*, H.S.Saini, Ed., Springer, 2019, pp. 229-239.

[13] F. Hussain and M. Qi, "Integrated Privacy Preserving Framework for Smart Home," 14th International Conference on Natural Computation, Fuzzy Systems and Knowledge Discovery (ICNC-FSKD), pp. 1246-1253, 2018.

[14] L. Xiao, X. Wan, L. Xiaozhen, Z. Yanyong and W. Di, "IoT Security Techniques based on Machine Learning: How do IoT Devices use AI to Enhance Security?," *IEEE Signal Processing Magazine*, vol. 35, no. 5, pp. 41-49, 2018.

[15] J. Melnick, "Top 10 Most Common Types of Cyber Attacks," Netwrix Blog, 2020. [Online]. Available from: https://blog.netwrix.com/2018/05/15/top-10-most-common-types-of-cyber-attacks/#Eavesdropping%20attack [retrieved: February, 2021]

[16] L. Xiao, Y. Li, G. Han, G. Liu and W. Zhuang, "PHY-Layer Spoofing Detection with Reinforcement Learning in Wireless Networks," IEEE Trans. Vehicular Technology, vol. 65, no. 12, pp. 10037-10047, 2016.

[17] C. N. Klokmose, M. Korn and H. Blunck, "WiFi Proximity Detection in Mobile Web Applications," p. 123–128, 2014.

[18] I. P. Mavridis, A.-I. E. Androulakis, A. B. Halkias and P. Mylonas, "Real-life Paradigms of Wireless Network Security Attacks," 15th Panhellenic Conference on Informatic, pp. 112-116, 2011.

[19] G. J. Brajones, C. J. Murillo, J. F.V. Valdés and L. F. Valero, "Detection and Mitigation of DoS and DDoS Attacks in IoT-Based Stateful SDN: An Experimental Approach," *Sensors* , vol. 20, no. 3, pp. 1-18, 03 02 2020.

[20] A. K. Sikder, G. Petracca, H. Aksu, T. Jaege and U. Selcuk, "A Survey on Sensor-based Threats to Internet-of-Things (IoT) Devices and Applications," vol. 30, no. 3, pp. 291-319, 2018.

[21] N. Apthorpe, D. Reisman and N. Feamster, "A Smart Home is No Castle: Privacy Vulnerabilities of Encrypted IoT Traffic," ArXiv Cryptography and Security, vol. abs/1705.06805, 2017.

[22] T. Nguyen, D. Nguyen, B. Tran, H. Vu and N. Mittal, "A Lightweight Solution for Defending Against Deauthentication/Disassociation Attacks on 802.11 Networks," *IEEE* , pp. 185-190, 2008.

[23] R. Trimananda et al., "Vigilia: Securing Smart Home Edge Computing," *Third ACM/IEEE Symposium on Edge Computing*, pp. 74-89, 2018.

[24] S. Hornick, S. Santhanam, A. Hill and S. B. Krous, "How Smart Speakers will Reinvent Travel," 2018. [Online]. Available:https://www.oliverwyman.com/our-expertise/insights/2018/sep/oliver-wyman-transport-and-logistics-2018/how-smart-speakers-will-reinvent-travel.html. [retrieved: February, 2021]

[25] Household Hacker, "How To Turn Your Phones Into WiFi Security Cameras", https://www.youtube.com/watch?v=y7h8L2zeLdE [retrieved: March, 2021]

[26] H. Luijten, "Use your old iPhone as a Security Camera (IP Camera)", https://www.tweaking4all.com/mobile-devices/ios/repurpose-old-ios/old-iphone-as-ip-camera/#related [retrieved: March, 2021]

 ISBN: 978-1-61208-837-2

A Comparative Study of Performance Analysis of Empirical Propagation Models for NB-IoT Protocol in Suburban Scenarios

Francine Cássia de Oliveira
INATEL
National Institute of Telecommunications
Santa Rita do Sapucaí, Brazil
e-mail: francine.cassia@mtel.inatel.br

José Marcos Câmara Brito
INATEL
National Institute of Telecommunications
Santa Rita do Sapucaí, Brazil
e-mail: brito@inatel.br

***Abstract*— Among the protocols available for Internet of Things (IoT) applications, the Narrow Band-Internet of Things (NB-IoT) is one of the most relevant for presenting advantages, such as long range, low latency and low energy consumption. One of the points questioned for every protocol is the ability to serve applications that are in a mobile environment. To validate the possibility of the protocol working in this scenario, it is necessary to evaluate its performance in different propagation environments. This article presents field measurements that were made on an NB-IoT operational network in a suburban environment. The measurement results were compared with the results calculated on three propagation models used to predict loss of propagation in a mobile environment: Cost-231 Hata, ITU-1225 and Erceg Greenstein. Comparisons show that the Cost-231 Hata model offers the best performance in predicting propagation loss in the considered scenarios. These results provide relevant information about the performance of the propagation models used, applied to the NB-IoT protocol in a suburban environment.**

Keywords-IoT; NB-IoT; Performance Analysis; Propagation Models.

I. INTRODUCTION

A. Background

The heterogeneous characteristics of communications between things introduce considerable challenges to the networks that are part of these new scenarios, including scalability, different traffic volumes, and Quality of Service (QoS) requirements. The requirements of the applications used by these devices can also vary from the sending of information with extremely low latency to the establishment of highly reliable and prioritized communication. The IoT networks should allow the communication of specific data rate and low complexity to meet all these critical requirements of the devices. There are also variations in coverage, where there is a possibility of areas with a radius from one meter to more than one kilometer [1].

Low Power Wide Area Network (LPWAN) networks were designed to meet long-range coverage applications. There are solutions proposed to work in unlicensed bands, like LoRA and SigFox [2][3], and others to operate in mobile communications bands, such as NB-IoT, which was designed to work with Long Term Evolution (LTE) [4].

NB-IoT is a promising technology developed to support massive implementations with low data rates and narrow bandwidth [5]. It also offers low-cost devices, battery life of more than ten years, and great capacity [6]. It can be deployed in three different modes: (i) stand-alone, as a dedicated carrier (200KHz channel), (ii) in-band, within the occupied bandwidth of a Physical Resource Block (PRB) carrier - 180KHz, and (iii) within a guarding period in the LTE carrier (PRB - 180KHz) [7]. It is interesting to note that the third mode presented allows NB-IoT support with minimal impact on LTE [8]. Figure 1 presents the joint NB-IoT operation with the LTE structure.

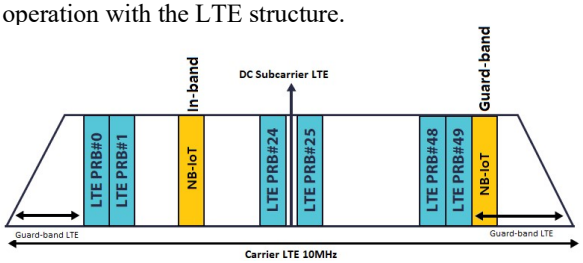


Figure 1. Operation Mode in-band and out-band.

The highest modulation scheme considered in NB-IoT is the Quadrature Phase Shift Keying (QPSK) [5], and only Frequency Duplexing Division mode (FDD) is supported. The multiple access scheme is identical to the LTE, i.e., Orthogonal Frequency Division Multiple Access (OFDMA) and Single Carrier - Frequency Division Multiple Access (SC-FDMA) for downlink and uplink, respectively. In downlink transmission, only one PRB is used, whereas, in the uplink, there are two options: single-tone transmission and multi-tone transmission. In single-tone, the spacing between subcarriers can be 3.75KHz or 15KHz [9]. Multi-tone enables sets of 3, 6, or 12 subcarriers. LTE's protocols are used in totality by NB-IoT users, and five new physical channels should be introduced. A new category of user equipment, called Cat-N, came with NB-IoT [10]. In addition to operating in LTE bands, NB-IoT can also work on the Global System for Mobile Communications (GSM), which is seen as a significant advantage since GSM already has global coverage. In this case, the signal is transmitted in

 ISBN: 978-1-61208-837-2

standalone mode [4] and operates with 200kHz bandwidth, the same as in GSM [11].

The range of NB-IoT technology is around 15 km, and the loss of extended coupling is approximately 20dB [7]. The operating frequencies available for NB-IoT are the same for LTE.

B. Motivation

Comparative analyses between real environments and empirical propagation models prove to be quite relevant for different protocols and technologies. They have a significant contribution to network planning and performance analysis of the adopted parameters [14].

Unlike protocols that operate in unlicensed frequency bands, protocols based on mobile communications networks, such as NB-IoT, are promising technologies developed to support massive deployments, with reduced data rates and narrow bandwidth [6]. However, their performance in mobile environments is not widely explored.

The main objective of this study is to analyze the performance of the NB-IoT protocol. The chosen scenario was the suburban mobile environment in the city of Santa Rita do Sapucaí, Minas Gerais - Brazil, using the network installed by the operator TIM (Telecom Italia Mobile). The main goal is, based on field measuremts (using a Quectel test device BG96), to find the best propagation model to characterize the network's performance.

C. Paper Organization

The remainder of this paper is organized as follows. Section II summarizes the related work. Section III presents the propagation models considered in our analysis. Section IV presents the conditions of field measurements. Section V focuses on the performance analysis of the results. Section VI concludes the paper and suggests future works.

II. Related Work

Several studies involving the performance of the NB-IoT protocol have been carried out to trace its performance in different scenarios. Also, comparative analyses between real environments and empirical propagation models prove to be quite relevant for different protocols and technologies as they have a significant contribution to network planning and performance analysis of the adopted parameters [14]. Ravi et al. [15] present the results obtained through experimental measurements to analyze the attenuation suffered in NB-IoT in indoor environments. According to Shin et al. [16], there are still many open problems concerning the link adaptation, performance analysis, and project optimization of the NB-IoT. A study of the NB-IoT performance is presented by Adhikary et al. [17] with an analysis of the different NB-IoT channels in various scenarios, considering the Typical Urban (TU) channel model, however, in a static environment, without mobility. Finally, Ingabire et al. [18] present a comparative study between the LoRaWAN coverage and the Okumura-Hata, Cost 231-Hata, Extended-Hata, and ITU-R 1225 propagation models in a static urban environment.

The related work present analyzes the NB-IoT protocol, as well as its advantages and behavior analysis in certain scenarios. And there is a similar analysis that relates the LoRaWAN protocol to propagation models.

III. Propagation Models

This section summarizes three propagation models used for this study: Cost-231 Hata, ITU-R 1225, and Erceg Greenstein models.

A. Cost-231 Hata Model

This model is an extension of the Okumura Hata model [19]. It is valid for frequencies between 500 MHz and 2000 MHz and can be applied in urban, suburban, and rural settings. The path loss is computed using the expressions below [20]:

$$PL\ (dB) = A + B\log(d) + C \quad (1)$$

where:

$$A = 46.3 + 33.9\log10(fc) - 13.28\log(hb) - a(hm) \quad (2)$$

fc is the frequency (MHz)
hb is the base station antenna height (m)
$a(hm)$ for urban scenarios is defined as:

$$a(hm) = 3.2(\log(11.75hr))^2 - 4.97 \quad (3)$$

hr is the device height (m)
$a(hm)$ for suburban scenarios is defined as:

$$a(hm) = (1.1\log(fc) - 0.7)hr - (1.56\log(fc)*0.8) \quad (4)$$

$$B = 44.9 - 6.55\log10(hb) \quad (5)$$

C = 0 for medium city and suburban areas and
C = 3 for metropolitan areas

B. ITU-R 1225 Model

Defined by the International Telecommunication Union - Radiocommunication Sector (ITU-R) [21], this empirical and semi-deterministic model can be used in urban and suburban scenarios and was designed for frequencies around 2000 MHz. In this model, the path loss is computed by (6).

$$PL\ (dB) = 40\log(d) + 30\log(f) + 49 \quad (6)$$

where d is the distance in kilometer and f is the frequency in MHz.

C. Erceg Greenstein

Erceg Greenstein is a statistical model derived from experimental data collected in the United States in 95 macrocells. This model is applicable in suburban scenarios

 ISBN: 978-1-61208-837-2

and has different categories for different terrain types [22]. The path loss in this model is computed by (7).

$$PL\ (dB) = A + 10\gamma\log(d/d0) + Xf + Xh \quad (7)$$

where;

$$A = 20\log(4\pi d0/\lambda) \quad (8)$$

$$\gamma = a - b*(hb) + c/hb \quad (9)$$

d = distance between the device and base station (m)
$d0$ = 100m
hb is the base station antenna height (m)

$$Xf = 6\log(fMhz/2000) \quad (10)$$

The parameter Xh is related to the type of terrain (A, B or C). Terrain A refers to hilly/moderate-to-heavy tree density. Terrain B refers to hilly/light tree density or flat/moderate-to-heavy tree density. Terrain C refers to flat/light tree density.

For terrain types A and B:

$$Xh = -10.8\log(hm/2) \quad (11)$$

For terrain type C:

$$Xh = -20\log(hm/2) \quad (12)$$

where;

h is the device antenna height (m)

Also, parameters a, b and c are related to the type of terrain and are described in Table 1.

TABLE I. PARAMETERS TO DIFFERENT TYPES OF TERRAIN

Parameter	Terrain A	Terrain B	Terrain C
a	4.6	4	3.6
b, m^{-1}	0.0075	0.0065	0.005
c, m	12.6	17.1	20

The choice for these models was based on the possibility of use in environments with mobility and on the similarity in the construction characteristics of each one, which include frequency, distance between the mobile device and the tower, height of the device, height of the tower, among others.

IV. FIELD TEST MEASUREMENTS

The scenario used in carrying out the measurements has a suburban profile with small obstructions caused by some low-rise buildings and constructions. The relief variation is approximately 50 meters. Routes that could totally obstruct the signal were avoided to prevent incorrect interpretations of the results, and the route layout also considered the need to repeat the experiment several times. It is important to note that an experiment refers to the round trip of the specified route. Twenty experiments were carried out on three routes within the city of Santa Rita do Sapucaí, and one route on the BR-459 highway in order to validate the behavior of the protocol at higher speeds, totaling the collection of 3000 samples.

All routes started at the same location, a few meters from the tower where the transmitting antenna was installed.

For route 1, the path was basically made in a straight line with some variations in altitude along the route.

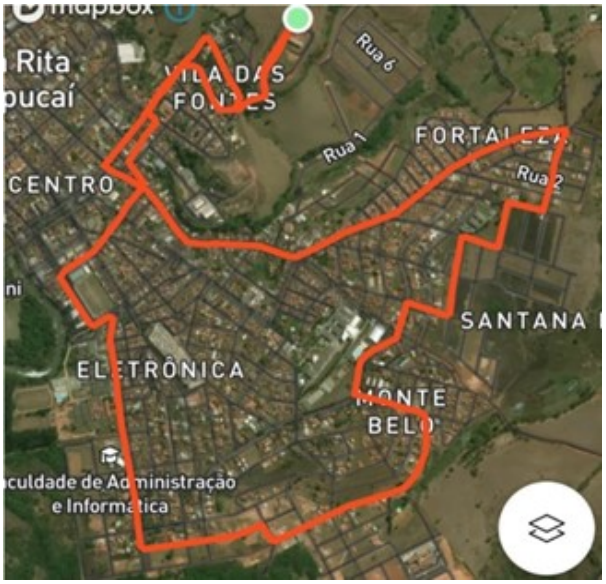
For route 2, the path traveled was crossing the city through the flatest part. The analyzed site presented residential buildings with no vegetation.

Route 3 was made in the part of the city where there were hills. The place had a certain density of vegetation, and residential buildings.

Finally, route 4 was carried out on the highway, having its format similar to route 1.

(a). Route 1.

(b). Route 2.



(c). Route 3.

Figure 2(d). Route 4.

As all routes presented similar characteristics with a certain density of vegetation and residential buildings, the environment was considered suburban.

The routes carried out within the city covered 11 km, 6.5 km and 8.7 km for routes 1, 2 and 3, respectively. For these, the average travel speed was 30 km/h. The route carried out on the highway covered 15 km, at speeds of 40km/h, 60 km/h and 80 km/h. Figures 2a, 2b, 2c, and 2d illustrate the routes used in the experiments.

A gateway Quectel model BG96 was used in the experiments. It is a wireless IoT communication module with LTE Cat M1, LTE Cat NB1, and General Packet Radio Services (EGPRS) functions. For the NB-IoT solution, the transmission power of the device is 23dBm. Also, it provides a Global Navigation Satellite System (GNSS).

The transmitting antenna information is in Table 2.

TABLE II. ANTENNA TRANSMITTING PARAMETERS

Parameter	Values
Frequency of operation (MHz)	1800
Polarization (º)	+/-45
Gain (dBi)	16.7
Horizontal Beamwidth (º)	68
Vertical Beamwidth (º)	7.0

We used a Universal Subscriber Identification Module (USIMCard) from the operator TIM. The base station is located on the top of the Cruzeiro hill in Santa Rita do Sapucaí.

V. PERFORMANCE ANALYSIS

In this section, the NB-IoT coverage will be analyzed along the four traced routes, and a comparison will be made with the three propagation models presented.

The conditions inserted in each propagation model for each route are presented in Table 3:

TABLE III. PROPAGATION MODELS PARAMETERS

Parameter	Values
Frequency of operation (MHz)	1800
Device antenna height (m)	1
Maximum distance between Tx and Rx (m)	4000
Basestation Antenna Height (m)	40

For each route, the measured values were compared with the values presented by the considered propagation models. The parameter used to represent the signal strength was the Received Signal Strength Indication (RSSI) [22] measured in dBm. The analytical expression for the theoretical RSSI values is presented below:

$$RSSI\ (dBm) = Pt + Gt + Gr - PL - A \qquad (13)$$

where;

Pt is the transmission power (dBm)
Gt is the transmission gain (dBi)
Gr is the reception gain (dBi)
PL is the Path Loss (dB)
A is the attenuation (dB)

Figure 3 compares the measured values of RRSI (samples) for one route and the values predicted by the propagation models.

To better interpret the measurements results, the measurement samples were grouped into clusters, with each cluster containing samples in a range between d - a and d + a, where d represents a given distance from the radio base.

 ISBN: 978-1-61208-837-2

After that, we computed the mean value of the RSSI, taking all samples belonging to the same cluster. Figures 4, 5 and 6 show the average RSSI measured and the RSSI computed using the propagation models for urban routes 1, 2, and 4. For route 3, the graph was not represented in this paper, because the results are similar to the of route 2.

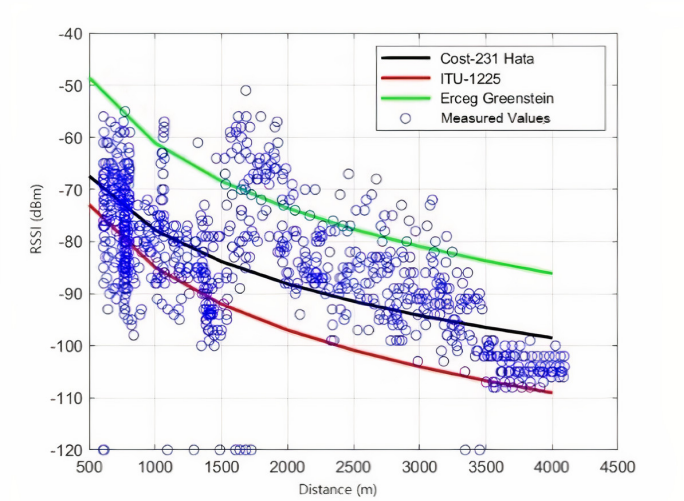


Figure 3. Measurements (samples) obtained in one route in comparison with the propagation models.

The behavior of the RSSI measurements are relatively similar in all these routes as the device moves away from the transmitting antenna.

Finally, Figure 7 shows the result of the average RSSI considering the samples of all routes.

Based on Figures 4, 5, 6, and 7, we can conclude that the Erceg Greenstein model is not accurate in predicting the propagation loss in the scenario considered in this paper.

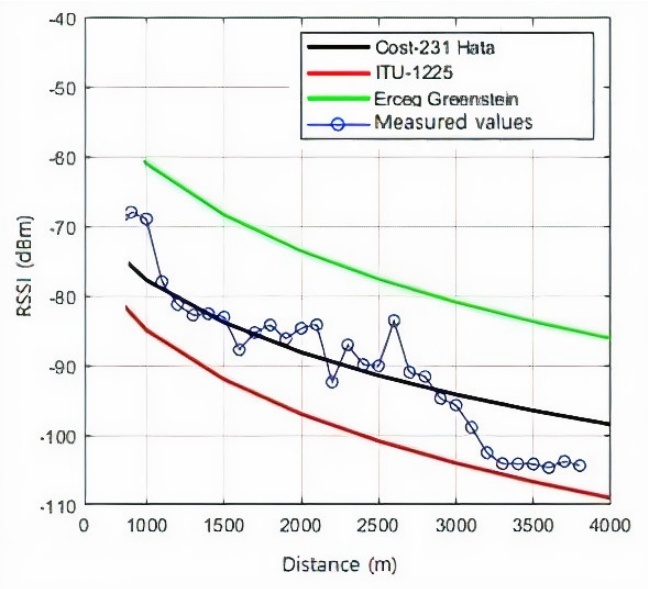


Figure 4. RSSI on the urban route 1.

The ITU-1225 model is adequate to predict the propagation loss for long distances on some routes. For short distances, the most accurate model is Cost-231 Hata. Also, when we grouped all measurements of all routes (Figure 7), the Cost-231 Hata model has the best performance.

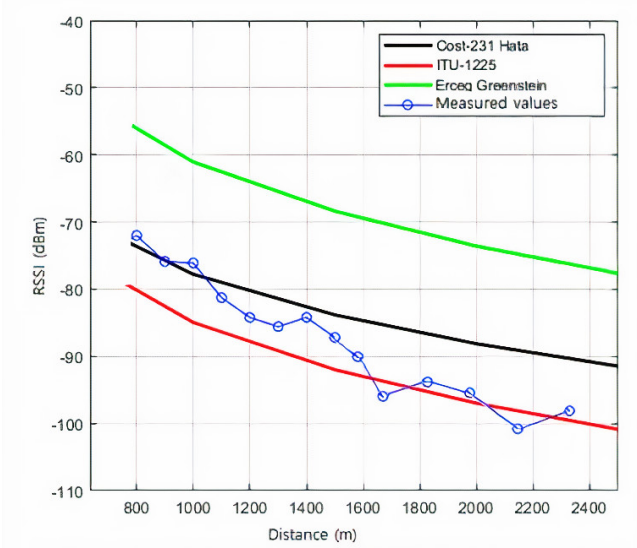


Figure 5. RSSI on the urban route 2.

In the route taken on the highway, the protocols behavior is different, and there is a sharp drop in the collection of samples after the distance of 2000m. As the average speed of travel of the device on this route is from 60 to 80 km/h, it is proved that the performance of NB-IoT in scenarios with mobility for medium to high speed is not efficient, which can impact the use of this protocol in mobile applications.

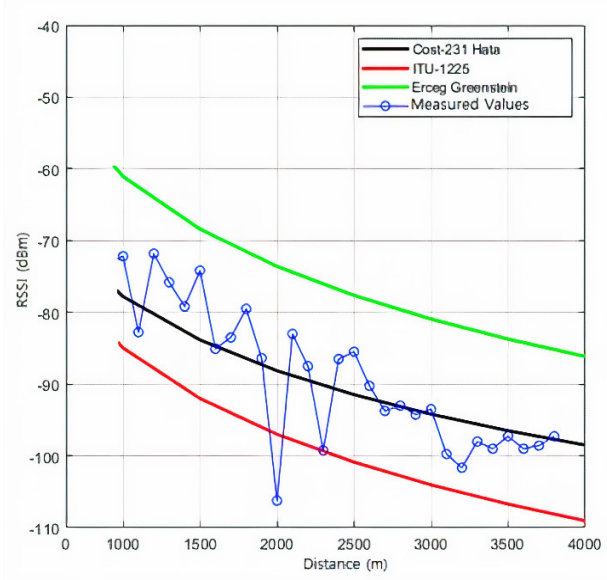


Figure 6. RSSI on the urban route 4.

 ISBN: 978-1-61208-837-2

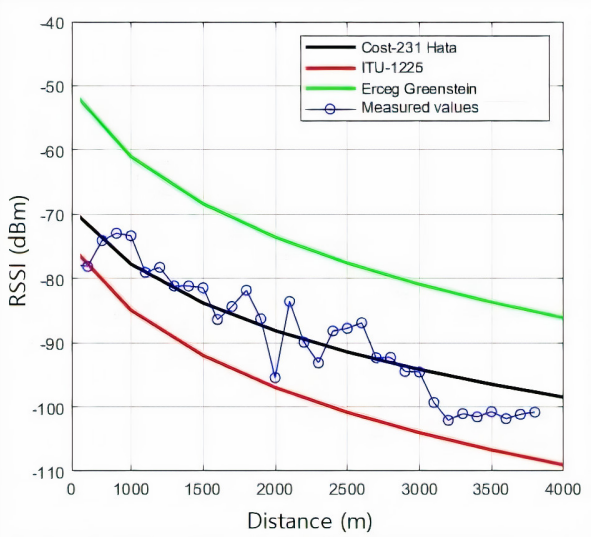


Figure 7. RSSI grouping all samples of all urban routes.

One key performance metrics used in evaluations is The Mean Absolute Error (MAE), which measures the average of all absolute errors between the measured values and the calculated results from the propagation models.

The performance of each propagation model is presented in Table 4.

TABLE IV. ERROR PERFORMANCE METRIC

Error Parameter	MAEs
Cost-231 Hata	3,588488
ITU-1225	8,568521
ERCEG GREENSTEIN	14,74494

According to the results, the Cost-231 Hata model has the lowest absolute mean error, confirming that this is the model that most closely matches the actual measured values.

VI. CONCLUSION AND FUTURE WORKS

In this paper, the NB-IoT protocol coverage was analyzed through real field measurements on four different routes in the city of Santa Rita do Sapucaí-MG, Brazil.

The measured results were compared with three propagation models used in mobile communication scenarios: Cost-231 Hata, ITU-R 1225, and Erceg-Greenstein.

The results presented by the Erceg-Greenstein model are not accurate for all considered routes. The ITU-R 1225 model has good performance for long distances on some routes. The best results are presented by the Cost-231 Hata model, which is confirmed using the MAE metric.

The protocol behaves differently on the route taken on the highway, and a stable communication link could not be established. Thus, the performance of NB-IoT for environments with medium to high speeds is not efficient.

The future works include analyses made with other protocols with characteristics similar to NB-IoT, such as LoRa, in the same scenarios and conditions, to compare the performance between both technologies.

ACKNOWLEDGMENT

This work was partially supported by RNP, with resources from MCTIC, Grant No. No 01245.010604/2020-14, under the 6G Mobile Communications Systems project of the Radiocommunication Reference Center (Centro de Referência em Radiocomunicações - CRR) of the National Institute of Telecommunications (Instituto Nacional de Telecomunicações - Inatel), Brazil.

REFERENCES

[1] K. Mekki, E. Bajic, F. Chaxel, and F. Meyer, “Overview of Cellular LPWAN Technologies for IoT Deployment : Sigfox, LoRaWAN, and NB-IoT”, IEEE International Conference on Pervasive Computing and Communications Workshops, pp. 197–202, 2018.

[2] LoRa-Alliance.org, “LoRa Alliance. LoRaWANTM101 - A Technical Introduction.” [Online]. Available: https://lora-alliance.org/resourcehub. [Accessed: 08-Mar-2021].

[3] S. Parkvall and E. Dahlman, “Evolution of LTE toward IMT-Advanced,” IEEE Communications Magazine, vol. 49, no.2, pp. 84–91, 2011.

[4] A. D. Zayas and P. Merino, “The 3GPP NB-IoT system architecture for the Internet of Things,” IEEE Int. Conf. Commun. Work. ICC Work. 2017, pp. 277–282, 2017.

[5] N. Mangalvedhe, R. Ratasuk, and A. Ghosh, “NB-IoT deployment study for low power wide area cellular IoT,” IEEE Int. Symp. Pers. Indoor Mob. Radio Commun. PIMRC, no. 1, pp. 92–97, 2016.

[6] R. Ratasuk, B. Vejlgaard, N. Mangalvedhe, and A. Ghosh, “NB-IoT system for M2M communication,” 2016 IEEE Wirel. Commun. Netw. Conf. Work. WCNCW 2016, no. Wd5g, pp. 428–432, 2016.

[7] R. Ratasuk, J. Tan, N. Mangalvedhe, M. H. Ng, and A. Ghosh, “Analysis of NB-IoT Deployment in LTE Guard-Band,” IEEE Veh. Technol. Conf., vol. 2017-June, pp. 17–21, 2017.

[8] H. Wang and A. O. Fapojuwo, “A Survey of Enabling Technologies of Low Power and Long Range Machine-to-Machine Communications,” IEEE Commun. Surv. Tutorials, vol. 19, no. 4, pp. 2621–2639, 2017.

[9] H. Malik et al., “Radio Resource Management Scheme in NB-IoT Systems,” IEEE Access, vol. 3536, pp. 15051-15064, 2018.

[10] M. Elsaadany, A. Ali, and W. Hamouda, “Cellular LTE-A Technologies for the Future Internet-of-Things: Physical Layer Features and Challenges,” IEEE Commun. Surv. Tutorials, vol. 19, no. 4, pp. 2544–2572, 2017.

[11] Y. D. Beyene et al., “NB-IoT Technology Overview and Experience from Cloud-RAN Implementation,” IEEE Wireless Communications., vol. 24, no. 3, pp. 26–32, 2017.

[12] J. Chebil, A. K. Lwas, R. Islam, and A. Zyoud, “Investigation of path loss models for mobile communications in Malaysia Investigation of Path Loss Models for Mobile Communications in Malaysia,” Australian Journal of Basic and Applied Sciences, pp. 365-371, 2011.

 ISBN: 978-1-61208-837-2

[13] K. M. Malarski et al., “Investigation of Deep Indoor NB-IoT Propagation Attenuation,” IEEE 90th Veh. Technol. Conf., pp. 1–5, 2019.

[14] A. Díaz-Zayas, C. A. García-Pérez, Á. M. Recio-Pérez, and P. Merino, “3GPP standards to deliver LTE connectivity for IoT,” IEEE 1st Int. Conf. Internet-of-Things Des. Implementation, IoTDI 2016, pp. 283–288, 2016.

[15] S. Ravi, P. Zand, M. El Soussi, and M. Nabi, “Evaluation, Modeling and Optimization of Coverage Enhancement Methods of NB-IoT,” IEEE 30th Annu. Int. Symp. Pers. Indoor Mob. Radio Commun., pp. 1–7, 2019.

[16] W. Shin, J. R. Lee, and H. H. Choi, “Energy-delay tradeoff analysis and enhancement in LTE power-saving mechanisms,” Dig. Tech. Pap. - IEEE Int. Conf. Consum. Electron., no. 1, pp. 11–12, 2013.

[17] A. Adhikary, X. Lin, Y. E. Wang, H. Way, and S. Jose, “Performance Evaluation of NB-IoT Coverage,” IEEE 84th Vehicular Technology Conference (VTC-Fall), pp. 1-5, 2016.

[18] W. Ingabire, H. Larijani, and R. M. Gibson, “Performance evaluation of propagation models for LoRaWAN in an urban environment,” International Conference on Electrical, Communication, and Computer Engineering (ICECCE), pp. 1368-1373, 2020.

[19] S. Sorooshyari, “Introduction to Mobile Radio Propagation and Characterization of Frequency Bands,” Wireless Communication Technologies, 16:332:559, 1996.

[20] Y. Singh, “Comparison of Okumura , Hata and COST-231 Models on the Basis of Path Loss and Signal Strength,” International Journal of Computer Applications, vol. 59, no. 11, pp. 37–41, 2012.

[21] “Guidelines for Evaluation of Radio Transmission Technology for IMT-2000.” [Online]. Available: https://www.itu.int/rec/R-REC-M.1225/en. [Accessed: 08-Mar-2021].

[22] V. Erceg et al., “An Empirically Based Path Loss Model for Wireless Channels in Suburban Environments,” IEEE Journal on Selected Areas in Communications, vol. 17, no. 7, pp. 1205–1211, 1999.

 ISBN: 978-1-61208-837-2

Dynamic Spectrum Sharing in Multi-Operator Millimeter-Wave Indoor Systems

Rony Kumer Saha
Radio and Spectrum Laboratory
KDDI Research, Inc.
2-1-15 Ohara, Fujimino-shi, Saitama, Japan
email: ro-saha@kddi-research.jp

***Abstract*—A Dynamic Spectrum Sharing (DSS) technique is presented, which allows dynamic access to the countrywide full 28 GHz Millimeter-Wave (mmWave) spectrum to an arbitrary number of Mobile Network Operators (MNOs) to serve their respective in-building Small Cells (SCs). Co-Channel Interference (CCI) is managed by controlling the transmission power of in-building SCs of each MNO. Using the Equal Likelihood Criterion and the properties of left-justified Pascal's triangle, we derive the system-level average capacity, Spectral Efficiency (SE), and Energy Efficiency (EE) performance metrics. We carry out numerical analyses and simulation results for a country with four MNOs. It is shown that the proposed DSS can improve SE by about 2.64 times and EE by about 74.28% over that of the Static Equal Spectrum Allocation (SESA). Moreover, we show that the proposed DSS requires the reuse of the countrywide mmWave spectrum to 71.87% fewer buildings of SCs than that required by the SESA to satisfy the expected SE and EE requirements for the Sixth-Generation (6G) mobile systems.**

Keywords—28 GHz; spectrum sharing; multi-operator; indoor; millimeter-wave; technique; small cell.

I. INTRODUCTION

Addressing high capacity and data rate demands with limited spectrum bandwidth allocated to a Mobile Network Operator (MNO) has become a major issue for the Fifth-Generation (5G) and beyond mobile systems. Since the achievable capacity is directly proportional to the spectrum bandwidth of an MNO, an effective approach to address high capacity and data rate is to allow each MNO to access the full spectrum in a country. However, allowing access to the Countrywide Full-Spectrum (CFS) to each MNO causes Co-Channel Interference (CCI), which can be managed in the Power-Domain (PD).

The concept of countrywide full spectrum allocation and sharing is not so obvious in the existing literature. Saha [1] proposed a hybrid interweave-underlay CFS allocation in the 28 GHz band by managing CCI in the PD. CFS allocation in the 28 GHz has been investigated later in Saha [2] by managing CCI in the time-and frequency-domain. However, in both studies, the analyses were limited to a specific number of MNOs in a country. In this paper, we relax the assumptions in Saha [1] and Saha [2] and present a Dynamic Spectrum Sharing (DSS) technique for an arbitrary number of MNOs in a country. Unlike the traditional DSS techniques in 5G New Radio (NR) where each MNO (allocated to a portion of the countrywide full spectra) shares its spectrum dynamically with other MNOs countrywide, the proposed DSS technique allows access to the countrywide full 28 GHz spectrum to each MNO dynamically to serve its in-building Small Cells (SCs) by controlling the transmission power of SCs within each building using the Equal Likelihood Criterion and the properties of left-justified Pascal's triangle.

We organize the paper as follows. In Section II, the system architecture and the proposed DSS technique are described. Relevant mathematical analysis of DSS is carried out in Section III and performance evaluation and comparison are performed in Section IV. We conclude the paper in Section V.

II. SYSTEM ARCHITECTURE AND PROPOSED DSS TECHNIQUE

A. System Architecture

The system architecture consists of an arbitrary number of O MNOs in a country, which is shown in Figure 1(a) for O=4. Considering a similar architectural feature for each MNO, only one MNO (e.g., MNO 1) is shown in detail in Figure 1(c). An SC of each MNO is deployed in each apartment of a building. All Macrocells (MCs) and Picocells (PCs) operate at the 2 GHz outdoors, while SCs operate at the 28 GHz indoors. Let P_{m} and P_{r} denote the maximum and the reduced transmission powers of an SC of MNO o. Since all MNOs operate at the CFS, with an increase in the number of interferers, i.e., SC User Equipments (SUEs) of MNOs $\boldsymbol{O}\backslash o$, the aggregate interference from one SC to another increases. This causes the transmission power P_{r} of each SC of all MNOs to be adjusted such that the aggregate interference power does not exceed the interference threshold (i.e., the maximum value of CCI power) I_{m}. Let $\alpha_1, \alpha_2, \ldots \alpha_{(|\boldsymbol{O}|-1)}$ denote scaling factors and $\alpha_1 > \alpha_2 > \cdots > \alpha_{(|\boldsymbol{O}|-1)}$ implying the percentages of P_{m} to adjust P_{r} such that $\sum_{x=1}^{(|\boldsymbol{O}|-1)} (\alpha_x \times P_{\mathrm{m}}) \le I_{\mathrm{m}}$. Figure 1(b) shows the transmission power levels of an SC to manage CCI for O=4. The existence of any interferer SUEs (iSUEs) of MNOs $\boldsymbol{O}\backslash o$ in an apartment can be detected by the SC of MNO o itself using any conventional spectrum sensing techniques to update the CCI and spectrum usage status real-time basis in every Transmission Time Interval (TTI) level by coordinating one MNO with another directly in a distributed manner [3].

B. Proposed DSS Technique

The proposed Dynamic Spectrum Sharing (DSS) technique is stated as follows. An MNO o can be allocated to the CFS dynamically to operate its in-building SCs, subjected to managing CCI with SCs of other MNOs $\boldsymbol{O}\backslash o$ over a certain license renewal term t_{r}. CCI is considered managing in the PD

 ISBN: 978-1-61208-837-2

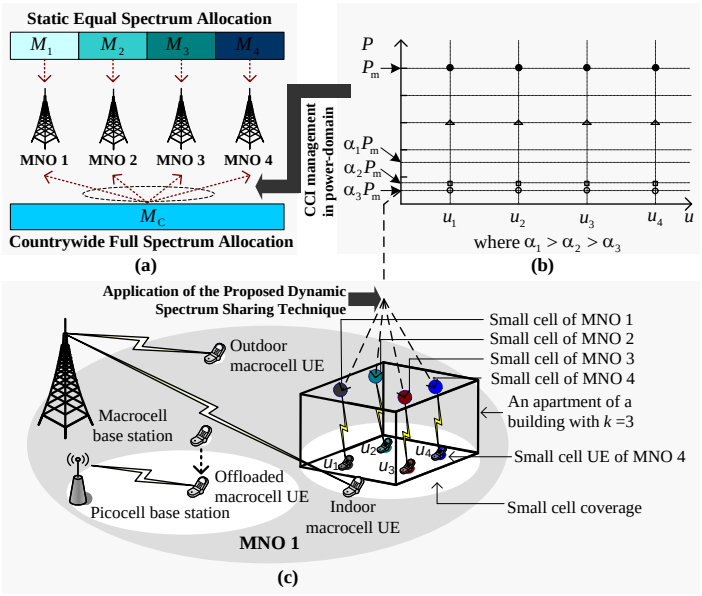


Figure 1. (a) Static Equal Spectrum Allocation (SESA) and CFS allocation. (b) Transmission power levels of an SC to manage CCI. (c) System architecture with 4 MNOs in a country.

by controlling the transmission power of each SC using the following principle. An SC of MNO o operates at the maximum transmission power if no SC User Equipment (UE) of MNOs $\boldsymbol{O}\backslash o$ is present, while at reduced power if an SUE of MNO $\boldsymbol{O}\backslash o$ is present, within the corresponding SC coverage of MNO o in a building. The reduced power is subjected to satisfying the maximum allowable CCI at the SC of MNO o.

III. Mathematical Analysis of DSS

Let O be the maximum number of MNOs in a country such that $o \in \boldsymbol{O} = \{1,2,...,O\}$. Let the amount of Millimeter-Wave (mmWave) spectrum allocated to an MNO o and a country, respectively, be M_o and M_{C}, defined in terms of the number of Resource Blocks (RBs) where an RB is equal to 180 kHz. Consider that each SC can serve one SUE at a time, and each combination of the coexistence of SUEs of MNOs $\boldsymbol{O}\backslash o$ (one UE from each MNO) with a UE of MNO o in an apartment is equally likely over any observation time $|\boldsymbol{T}| = Q$ and hence occurs with a probability of $\left(Q/2^{O-1}\right)$. Let k be a set of positive integers (representing the number of iSUEs of MNOs $\boldsymbol{O}\backslash o$ in an apartment) such that $0 \le k \le \left(|\boldsymbol{O}|-1\right)$. Then, the duration of an SC of MNO o corresponding to k can be defined by the Binomial coefficients $\mathbf{C}(O-1,k)$ of row $(O-1)$ of the left-justified Pascal's triangle [4] as follows.

$$t_{o,k} = \mathbf{C}(O-1,k)\left(Q/2^{O-1}\right) \tag{1}$$

Assume that $\boldsymbol{U}_o$ denotes a set of iSUEs of MNOs $\boldsymbol{O}\backslash o$ for an SC of MNO o such that $u_o \in \boldsymbol{U}_o = \{\boldsymbol{O}\backslash o\}$. Let P_{m} and P_{r} denote the transmission powers of an SC of MNO o corresponding to $|\boldsymbol{U}_o| = 0$ and $|\boldsymbol{U}_o| > 0$, respectively, such that P_{r} can be adjusted as follows.

$$P_{\mathrm{r}} = \begin{Bmatrix} \alpha_1 P_{\mathrm{m}}, & \text{for } |\boldsymbol{U}_o| = 1 \\ \vdots & \vdots \\ \alpha_{(|\boldsymbol{O}|-1)} P_{\mathrm{m}}, & \text{for } |\boldsymbol{U}_o| = \left(|\boldsymbol{O}|-1\right) \end{Bmatrix} \tag{2}$$

Using Shannon's capacity formula, a link throughput at RB=i in TTI=t for an MNO o in bps per Hz is given by

$$\sigma_{o,t,i}\left(\rho_{o,t,i}\right) = \begin{Bmatrix} 0, & \rho_{o,t,i} < -10\,\mathrm{dB} \\ \beta \log_2\left(1+10^{\left(\rho_{o,t,i}(\mathrm{dB})/10\right)}\right), & -10\,\mathrm{dB} \le \rho_{o,t,i} \le 22\,\mathrm{dB} \\ 4.4, & \rho_{o,t,i} > 22\,\mathrm{dB} \end{Bmatrix}$$

where $\rho_{o,t,i}$ denotes Signal-to-Interference-plus-Noise-Ratio (SINR) at RB=i in TTI=t for an MNO o in dB. β denotes the implementation loss factor.

Let P_{MC} and P_{PC} denote the transmission power of an MC and a PC, respectively, and $S_{\mathrm{M},o}$ and $S_{\mathrm{P},o}$ denote the number of MCs and PCs, respectively, of MNO o. Let M_o^{MC} denote the spectrum of an MC of MNO o. The average capacity of an MC of MNO o can be given as follows where σ and ρ are responses over M_o^{MC} RBs in $t \in \boldsymbol{T}$.

$$\sigma_o^{\mathrm{MC}} = \sum_{t \in \boldsymbol{T}} \sum_{i=1}^{M_o^{\mathrm{MC}}} \sigma_{o,t,i}\left(\rho_{o,t,i}\right) \tag{3}$$

However, due to the presence of Line-Of-Sight (LOS) components, low multipath fading effect, high distance-dependent path loss, small coverage, high wall and floor penetration loss, and low UE speed, the signal propagation characteristic at a high-frequency 28 GHz mmWave band does not change considerably indoors. Hence, we consider that each building has similar indoor signal propagation characteristics.

 ISBN: 978-1-61208-837-2

Then, by linear approximation, the average capacity, Spectral Efficiency (SE), and Energy Efficiency (EE) of all MNOs each with S_F SCs per building for the proposed DSS can be given, respectively, for L buildings by,

$$\sigma_{\mathrm{DSS}}^{\mathrm{CA}} = \sum_{o=1}^{O}\left(\sigma_o^{\mathrm{MC}} + \left(\sum_{l=1}^{L}\sum_{s=1}^{S_F}\sum_{k=0}^{O-1}\left(\sum_{t=1}^{\left(\mathbf{C}(O-1,k)\left(\frac{Q}{2^{O-1}}\right)\right)}\sum_{i=1}^{M_C}\sigma_{o,k,t,i}\left(\rho_{o,k,t,i}\right)\right)\right)\right) \quad (4)$$

$$\sigma_{\mathrm{DSS}}^{\mathrm{SE}} = \sigma_{\mathrm{DSS}}^{\mathrm{CA}} \Big/ \left(\left(M_{\mathrm{C}} + \sum_{o=1}^{O} M_o^{\mathrm{MC}}\right)\times Q\right) \quad (5)$$

$$\sigma_{\mathrm{DSS}}^{\mathrm{EE}} = \frac{\sum_{o=1}^{O}\left(\sum_{l=1}^{L}\left(\begin{matrix}\left(P_{\mathrm{m}}/2^{O-1}\right)+\\ \sum_{k=1}^{(|\mathbf{o}|-1)}\left(\begin{matrix}\mathbf{C}(O-1,k)\\ \left((\alpha_k P_{\mathrm{m}})/2^{O-1}\right)\end{matrix}\right)\end{matrix}\right)+\left(\begin{matrix}S_{\mathrm{P},o}P_{\mathrm{PC}}+\\ S_{\mathrm{M},o}P_{\mathrm{MC}}\end{matrix}\right)\right)}{\left(\sigma_{\mathrm{DSS}}^{\mathrm{CA}}/Q\right)} \quad (6)$$

In SESA, let each MNO be allocated to an equal amount of spectrum of M RBs. The system-level average capacity, SE, and EE of all MNOs for SESA can be given, respectively, by

$$\sigma_{\mathrm{SESA}}^{\mathrm{CA}} = \sum_{o=1}^{O}\left(\sigma_o^{\mathrm{MC}} + \sum_{l=1}^{L}\left(\sum_{s=1}^{S_F}\sum_{t\in\boldsymbol{T}}\sum_{i=1}^{M}\sigma_{o,l,s,t,i}\left(\rho_{o,l,s,t,i}\right)\right)\right) \quad (7)$$

$$\sigma_{\mathrm{SESA}}^{\mathrm{SE}} = \sigma_{\mathrm{SESA}}^{\mathrm{CA}} \Big/ \left(\left(M_{\mathrm{C}} + \sum_{o=1}^{O} M_o^{\mathrm{MC}}\right)\times Q\right) \quad (8)$$

$$\sigma_{\mathrm{SESA}}^{\mathrm{EE}} = \sum_{o=1}^{O}\left(\begin{matrix}\sum_{l=1}^{L}\sum_{s=1}^{S_F}P_{\mathrm{m}}+\\ \left(S_{\mathrm{P},o}P_{\mathrm{PC}}\right)+\left(S_{\mathrm{M},o}P_{\mathrm{MC}}\right)\end{matrix}\right) \Big/ \left(\sigma_{\mathrm{SESA}}^{\mathrm{CA}}/Q\right) \quad (9)$$

IV. Performance Evaluation and Comparison

Table I shows selected parameters and assumptions used for the performance evaluation. However, the detailed simulation parameters and assumptions can be found in [2]. Using (4)-(9) and Table I, Figure 2 shows average capacity, SE, and EE responses for the proposed DSS and traditional SESA techniques. From Figure 2(a), it can be found that proposed DSS improves SE by about 2.64 times and EE by about 74.28%, respectively over that of the traditional SESA. The similar outperformance in SE and EE can be found in Figures 2(b)-2(c) over that of SESA with the variation of L.

TABLE I. DEFAULT PARAMETERS AND ASSUMPTIONS

Parameters and Assumptions	Value
Spectrum bandwidth	200 MHz (28 GHz) and 40 MHz (2 GHz)
Number of MNOs, Transmission direction	4, downlink
P_{m} , CCI threshold, SCs per building	19 dBm, $0.3P_{\mathrm{m}}$, 48

The Sixth-Generation (6G) mobile system is expected to offer SE of 370 bps/Hz and EE of 0.3 uJ/bit [5]. Using Figure 2(b), the minimum values of L required by DSS and SESA are 9 and 32, respectively, to satisfy the above SE and EE requirements for 6G. Hence, DSS requires the reuse of the countrywide 28 GHz spectrum to 71.87% fewer buildings than that of SESA.

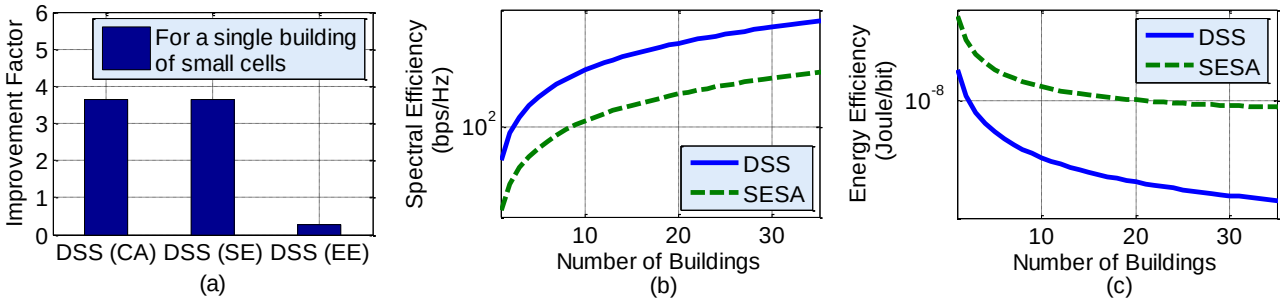


Figure 2. (a) Average capacity, SE, and EE improvement factors of DSS over that of SESA for L=1. (b) SE and (c) EE of DSS and SESA techniques for L>1.

V. Conclusion

In this paper, we have presented a Dynamic Spectrum Sharing (DSS) technique to share the countrywide full 28 GHz spectrum with in-building SCs of each MNO by controlling the transmission power of SCs. The proposed DSS has been detailed, and its outperformance over the traditional SESA in terms of average capacity, SE and, EE has been shown.

References

[1] R. K. Saha, "Licensed Countrywide Full-Spectrum Allocation: A New Paradigm for Millimeter-Wave Mobile Systems in 5G/6G Era," IEEE Access, vol. 8, pp. 166612-166629, 2020, doi: 10.1109/ACCESS.2020.3023342.

[2] R. K. Saha, "A Hybrid Interweave-Underlay Countrywide Millimeter-Wave Spectrum Access and Reuse Technique for CR Indoor Small Cells in 5G/6G Era," Sensors, 2020, vol. 20, Art. No. 3979, pp. 1-20 July 2020, doi: 10.3390/s20143979.

[3] R. H. Tehrani, S. Vahid, D. Triantafyllopoulou, H. Lee and K. Moessner, "Licensed Spectrum Sharing Schemes for Mobile Operators: A Survey and Outlook," IEEE Commun. Surv. Tuts., vol. 18, no. 4, pp. 2591-2623, Fourth quarter 2016, doi: 10.1109/COMST.2016.2583499.

[4] G Kallós, "A Generalization of Pascal's Triangle using Powers of Base Numbers," Annales Mathematiques Blaise Pascal, vol. 13, pp. 1-15, 2006.

[5] S. Chen et al., "Vision, Requirements, and Technology Trend of 6G: How to Tackle the Challenges of System Coverage, Capacity, User Data-Rate and Movement Speed," IEEE Wirel. Commun., vol. 27, no. 2, pp. 218-228, April 2020, doi: 10.1109/MWC.001.1900333.

 ISBN: 978-1-61208-837-2

Spectrum Reuse in the Terahertz Band for In-building Small Cell Networks

Rony Kumer Saha
Radio and Spectrum Laboratory
KDDI Research, Inc.
2-1-15 Ohara, Fujimino-shi, Saitama, Japan
email: ro-saha@kddi-research.jp

***Abstract*—In this paper, we present an analytical model to reuse spectrum in the Terahertz (THz) band in small cells located within a building. We characterize Co-Channel Interference (CCI) in the 140 GHz band and derive a minimum distance between co-channel small cells subject to satisfying predefined CCI interference constraints in both intra-floor and inter-floor levels. The set of small cells in both intra-floor and inter-floor levels constitute a 3-Dimensional (3D) cluster of small cells. The whole THz spectrum allocated to a Mobile Network Operator (MNO) can be reused to small cells of each cluster. We derive system-level average capacity, Spectral Efficiency (SE), and Energy Efficiency (EE) metrics for an arbitrary number of *L* buildings of small cells located over a macrocell coverage. With extensive numerical and simulation results and analyses, we show that the 3D clustering of small cells in a building and reusing the same spectrum in the 140 GHz band to each cluster improve both the SE and EE performances. Further, it is shown that the expected SE and EE requirements for the future Sixth-Generation (6G) mobile networks can be achieved by reusing the spectrum in a fewer number of buildings of small cells than that required when no spectrum reuse is considered.**

Keywords—6G; clustering; energy efficiency; in-building; small cell; spectral efficiency; spectrum reuse; THz band.

I. INTRODUCTION

Radio spectrum in mobile wireless communications is scarce and very costly. A direct, yet effective, way to improve the network capacity of a Mobile Network Operator (MNO) is to increase the system bandwidth by aggregating spectra in different bands. In this regard, due to the availability of large spectrum availability, high-frequency spectra in the range of millimeter-wave (mmWave) bands and Terahertz (THz) bands are considered to operate small cells deployed within a building. Even though, the Fifth-Generation (5G) mobile network has been rolled out in many countries in several mmWave spectrum bands, including 28 GHz and 39 GHz, the future Sixth-Generation (6G) is expected to operate in even higher frequencies such as THz bands. Due to their operational and signal propagation characteristics, including high distant-dependent path loss, low transmit power, small coverage, and presence of Line-Of-Sight (LOS) components, both mmWave and THz bands are suitable to serve indoor coverage.

Another major approach to improve the network capacity is to reuse the same spectrum spatially more than once. In this regard, due to high penetration losses from external and internal walls, as well as floors in a building, the high-frequency spectrum can be reused suitably by forming a 3-Dimensional (3D) cluster of small cells subject to managing Co-Channel Interference (CCI) between co-channel small cells. The whole spectrum can be reused to small cells per 3D cluster. However, comprehensive modeling of interference, as well as clustering of small cells, for reusing spectrum in them under the in-building scenario are not obvious. To the best of our knowledge, we first addressed these issues by modeling CCI and defining a minimum distance between co-channel small cells in a building in both intra-floor and inter-floor levels to develop a 3D cluster of small cells in order to reuse the same spectrum in each cluster in the 2 GHz microwave band Saha [1]. Likewise, in Saha [2], we dealt with managing CCI between co-channel small cells in the 28 GHz and 60 GHz mmWave bands to reuse both spectra in each 3D cluster of small cells. Due to considerable differences in operational requirements and signal propagation characteristics from the microwave and mmWave bands, following the continuation in Saha [1] and Saha [2], in this paper, we model CCI in the 140 GHz THz band to define a 3D cluster of in-building small cells in order to reuse the THz spectrum of an MNO in each 3D cluster.

In doing so, firstly, we discuss the system architecture and 140 GHz, indoor loss model, in Section II. We then present in brief CCI in both intra-floor level and inter-floor levels of a building and deduce minimum distances between co-channel small cells in both levels. A 3D cluster of small cells is then defined subject to satisfying both intra-floor and inter-floor interference constraints set by an MNO. The whole spectrum in the 140 GHz band is then reused to each 3D cluster of small cells. We derive system-level average capacity, Spectral Efficiency (SE), and Energy Efficiency (EE) metrics in Section III. In Section IV, we define parameters and assumptions, evaluate the impact of 3D clustering of in-building small cells, and compare the system-level SE and EE performances of the MNO with the corresponding expected requirements for the 6G mobile networks. We conclude the paper in Section V.

II. SYSTEM ARCHITECTURE AND THZ INDOOR LOSS MODEL

A. System Architecture

We consider a simple system architecture of an MNO, i.e., MNO 1, in a country as shown in Figure 1(a), which has three types of Base Stations (BSs), including Macrocell BS (MBS), Picocell BS (PBS), and Small cell BS (SBS). MBSs and PBSs operate in the 2 GHz spectrum, whereas all SBSs located in buildings are operated in the 140 GHz spectrum. Figure 1(a) also shows the placement of SBSs at the center of the ceiling of each apartment in a building. Each SBS serves one User Equipment (UE) at a time. An illustrative clustering in the inter-floor level (a single floor) and intra-floor level (nine

 ISBN: 978-1-61208-837-2

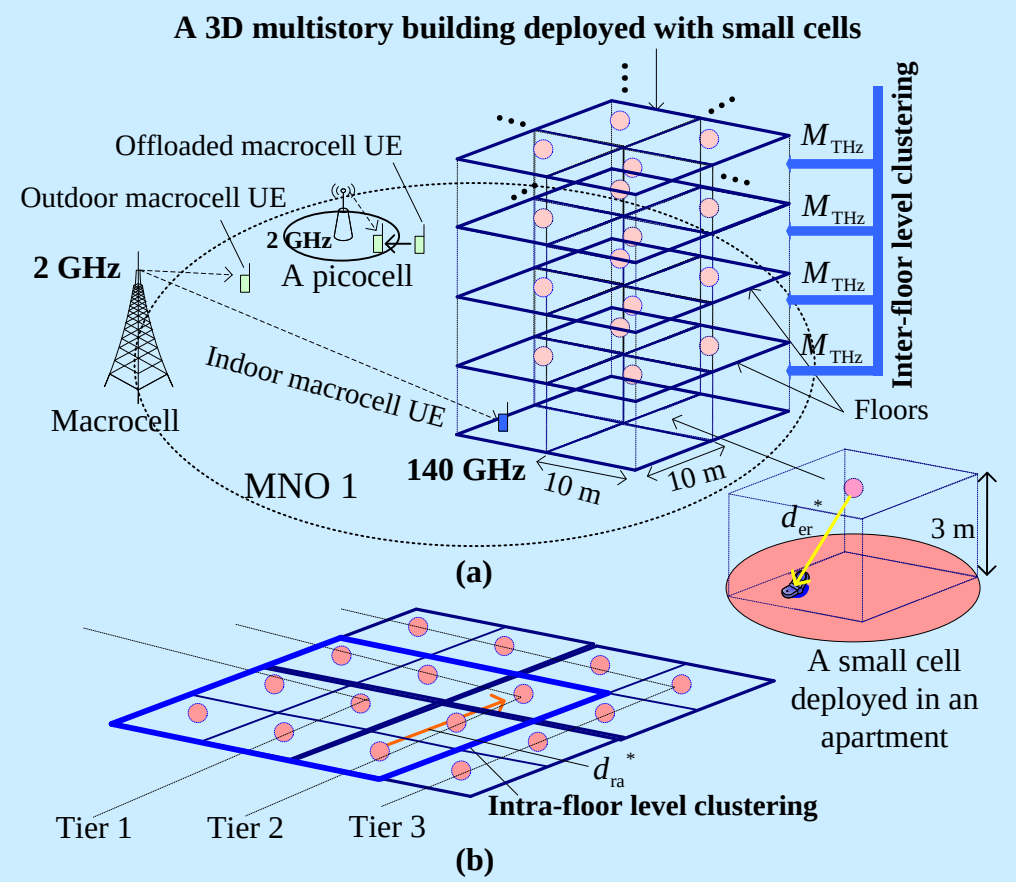


Figure 1. (a) an illustration of the system architecture of MNO 1 with a multistory building of small cells to reuse 140 GHz spectrum. (b) Intra-floor level clustering of small cells. Each circle represents a small cell in an apartment.

apartments) is shown in Figures 1(a) and 1(b), respectively. We discuss clustering in more detail in Section III.

B. 140 GHz Indoor Loss Model

1) Indoor path loss model: We consider the LOS path loss model for indoor THz communications in the 140-150 GHz band such that the average path loss at a distance d can be expressed as follows [3].

$$PL[d] = PL[d_o] + 10\gamma \log_{10}(d/d_0) + X_\Delta \quad (1)$$

where, $PL(d_0)$ denotes the path loss at the reference distance $d_0 = 0.35$ m (i.e., 0.5 m with 0.15 m is compensated for the waveguides [3]). X_Δ in dB is a zero-mean Gaussian distributed random variable with a standard deviation $\Delta = 0.5712$ dB. $\gamma = 2.117$ denotes path loss exponent [3].

Putting these above values in (1) $PL[d]$ can be expressed at the 140 GHz as follows and is proved in Proof 1.

$$PL[d] = 75.89 + 21.17 \log_{10}(d) + X_\Delta \quad (2)$$

Proof 1: We know, $PL[d_0] = 10\log_{10}(4\pi d_0 f/c)$

$$\gg PL[d_0] = 20\log_{10}(d_0) + 20\log_{10} f(\text{Hz}) - 147.55$$

$$\gg PL[d_0] = 32.44 + 20\log_{10}(d_0) + 20\log_{10} f(\text{GHz})$$

For $f = 140$ GHz, we can write the following.

$$\gg PL[d_0] = 32.44 + 20\log_{10}(d_0) + 20\log_{10}(140)$$

$$\gg PL[d_0] = 75.36 + 20\log_{10}(d_0)$$

Now, using (1), and putting $d_0 = 0.35$ m and $\gamma = 2.117$, we can find the following.

$$PL[d] = 75.36 + 20\log_{10}(0.35) + (10 \times 2.117)\log_{10}(d/0.35) + X_\Delta$$

$$PL[d] = 66.241 + 21.17\log_{10}(d) + 9.65 + X_\Delta$$

$$PL[d] = 75.89 + 21.17\log_{10}(d) + X_\Delta \quad \blacksquare$$

2) 140 GHz floor attenuation loss model: The floor penetration loss is not linear and decreases with an increase in the number of floors. Moreover, the floor attenuation loss is frequency-dependent and increases with an increase in frequency. In general, experimental signal propagation studies and results in the THz band are very limited in the existing literature. Hence, if we consider a reinforced concrete floor, according to [4], the floor attenuation loss is above 50 dB for

the first floor at 28 GHz. Since the floor attenuation loss increase with an increase in frequency, the loss at 140 GHz must be higher than 50 dB for the first floor. The impact of CCI at this floor attenuation loss of more than 50 dB for the first floor at the 140 GHz is negligible in the adjacent floor, and hence we assume no CCI interference effect from one adjacent floor to another at the 140 GHz band.

III. Modeling CCI, 3D Cluster, and Spectrum Reuse in 140 GHz Band and Estimating Performance Metrics

A. Modeling CCI, Small Cell Cluster, and Spectrum Reuse in the 140 GHz Band

1) Co-channel interference modeling: Following [2], the normalized CCI at a small cell UE in the intra-floor level and inter-floor level, respectively, can be given by,

$$\alpha_{\mathrm{ra}}\left(d_{\mathrm{ra}}\right)=\left(d_{\mathrm{m}}/d_{\mathrm{ra}}\right)^{2.117} \tag{3}$$

$$\alpha_{\mathrm{er}}\left(d_{\mathrm{er}}\right)=10^{-0.1\alpha_{\mathrm{f}}\left(d_{\mathrm{er}}\right)}\times\left(d_{\mathrm{m}}/d_{\mathrm{er}}\right)^{2.117} \tag{4}$$

where $\alpha_{\mathrm{f}}\left(d_{\mathrm{er}}\right)$ denotes floor penetration loss. d_{ra} and d_{er} denote, respectively, a minimum distance between co-channel small cells to allow reusing the same spectrum to both small cells. d_{m} defines a distance from small cells corresponding to the maximum CCI experienced by a small cell UE.

Proof 2: See Section II(C) of [2] for the Proofs of (3) and (4).

2) Minimum distance estimation: Let $I_{\mathrm{m,ra}}$ and $I_{\mathrm{m,er}}$ denote, respectively, the maximum number of co-channel interferers in the intra-floor and inter-floor levels. For square-grid apartments (Figure 1(a)) per floor of a multistory building, $I_{\mathrm{m,ra}}=8$ and $I_{\mathrm{m,er}}$ is 1 and 2, respectively, for the single-sided and double-sided co-channel interferers [2]. Now, let the optimal value of the aggregate CCI set by an operator in the intra-floor and inter-floor levels are denoted as $\alpha_{\mathrm{ra,op}}$ and $\alpha_{\mathrm{er,op}}$, respectively. Let at a minimum distance $d_{\mathrm{ra}}=d_{\mathrm{ra}}^{*}$ in the intra-floor level and $d_{\mathrm{er}}=d_{\mathrm{er}}^{*}$ in the inter-floor level, $\alpha_{\mathrm{ra,op}}$ and $\alpha_{\mathrm{er,op}}$ can be satisfied, i.e., the following conditions must satisfy.

$$I_{\mathrm{m,ra}}\times\left(d_{\mathrm{m}}/d_{\mathrm{ra}}\right)^{2.117}\le\alpha_{\mathrm{ra,op}} \tag{5}$$

$$I_{\mathrm{m,er}}\times\left(10^{-0.1\alpha_{\mathrm{f}}\left(d_{\mathrm{er}}\right)}\times\left(d_{\mathrm{m}}/d_{\mathrm{er}}\right)^{2.117}\right)\le\alpha_{\mathrm{er,op}} \tag{6}$$

After manipulating (5) and (6), the minimum distances in the intra-floor level and inter-floor level can be expressed as follows.

$$d_{\mathrm{ra}}^{*}\ge d_{\mathrm{m}}\times\left(I_{\mathrm{m,ra}}/\alpha_{\mathrm{ra,op}}\right)^{2.117^{-1}} \tag{7}$$

$$d_{\mathrm{er}}^{*}\ge d_{\mathrm{m}}\times\left(10^{-0.1\alpha_{\mathrm{f}}\left(d_{\mathrm{er}}\right)}\times\left(I_{\mathrm{m,er}}/\alpha_{\mathrm{er,op}}\right)\right)^{2.117^{-1}} \tag{8}$$

Proof 3: See Section III of [2] for the Proofs of (7) and (8).

3) Clustering and spectrum reuse factor: Let S_{ra} and S_{er} denote the maximum number of small cells corresponding to satisfying the minimum distances d_{ra}^{*} and d_{er}^{*}, respectively, such that the size of a 3D cluster of small cells deployed across intra-floor and inter-floor levels is given by,

$$S_{\mathrm{F}}=\left(S_{\mathrm{ra}}\times S_{\mathrm{er}}\right) \tag{9}$$

Hence, for a given number of small cells $S_{\mathrm{F,tot}}$ per building, the same THz spectrum band can be reused by the number of times (i.e., Spectrum Reuse Factor) per building of small cells as given below.

$$\varepsilon=S_{\mathrm{F,tot}}/S_{\mathrm{F}} \tag{10}$$

For more information on the clustering of small cells and reuse of the same spectrum in small cells within a building, please refer to [2].

B. Estimating Performance Metrics

Let M_{GHz} and M_{THz} denote, respectively, the number of Resource Blocks (RBs) in the 2 GHz spectrum and 140 GHz spectrum where an RB is equal to 180 kHz. Let $P_{\mathrm{GHz,MC}}$, $P_{\mathrm{GHz,PC}}$, and $P_{\mathrm{THz,SC}}$ denote, respectively, the transmission power of a macrocell, a picocell, and a small cell. Then, a link throughput at RB=i in a Transmission Time Interval (TTI)=t in bps per Hz corresponding to the downlink received signal-to-interference-plus-noise ratio $\rho_{t,i}$ is given by,

$$\sigma_{t,i}\left(\rho_{t,i}\right)=\begin{cases}0, & \rho_{t,i}<-10\,\mathrm{dB}\\ \beta\log_2\left(1+10^{\left(\rho_{t,i}(\mathrm{dB})/10\right)}\right), & -10\,\mathrm{dB}\le\rho_{t,i}\le 22\,\mathrm{dB}\\ 4.4, & \rho_{t,i}>22\,\mathrm{dB}\end{cases} \tag{11}$$

where β denotes the implementation loss factor. The total capacity of all macrocell UEs in $t\in\boldsymbol{T}=\{1,2,\ldots,Q\}$ is given by,

$$\sigma_{\mathrm{MC}}=\sum_{t=1}^{Q}\sum_{i=1}^{M_{\mathrm{GHz}}}\sigma_{t,i}\left(\rho_{t,i}\right) \tag{12}$$

Now, the aggregate capacity served by a small cell in a building in $t\in\boldsymbol{T}$ over M_{THz} RBs is given by,

$$\sigma_{s}=\sum_{t\in\boldsymbol{T}}\sum_{i=1}^{M_{\mathrm{THz}}}\sigma_{t,i}\left(\rho_{t,i}\right) \tag{13}$$

Since each 3D cluster of small cells consists of S_{F} small cells in a building, and the total 140 GHz spectrum can be reused to each cluster, the aggregate capacity served by a 3D cluster of small cells in $t\in\boldsymbol{T}$ over M_{THz} RBs is given by,

$$\sigma_{\mathrm{3D}}=\sum_{s=1}^{S_{\mathrm{F}}}\sigma_{s}$$

$$\sigma_{\mathrm{3D}}=\sum_{s=1}^{S_{\mathrm{F}}}\sum_{t\in\boldsymbol{T}}\sum_{i=1}^{M_{\mathrm{THz}}}\sigma_{t,i}\left(\rho_{t,i}\right) \tag{14}$$

 ISBN: 978-1-61208-837-2

Using (10), since there are ε 3D clusters of small cells per building, the same 140 GHz spectrum can be reused ε times to small cells per building. Hence, the aggregate capacity served by all small cells $S_{\mathrm{F,tot}}$, i.e., $(\varepsilon \times S_{\mathrm{F}})$, per building is given by,

$$\sigma_{\mathrm{THz}} = (\varepsilon \times \sigma_{\mathrm{3D}})$$

$$\sigma_{\mathrm{THz}} = \varepsilon \times \left(\sum_{s=1}^{S_{\mathrm{F}}} \sum_{t \in \boldsymbol{T}} \sum_{i=1}^{M_{\mathrm{THz}}} \sigma_{t,i} \left(\rho_{t,i} \right) \right) \quad (15)$$

Due to the high operating frequency and the low transmission power of each small cell, we consider similar indoor signal propagation characteristics for all *L* buildings per macrocell. Then, by linear approximation, the system-level average capacity per macrocell of MNO 1 is given by the sum of the aggregate capacity of all macrocell UEs served by the macrocell and picocells and the aggregate capacity of all small cell UEs served by small cells in *L* buildings. Hence, using (12) and (15), the system-level average capacity per macrocell of MNO 1 is given by

$$\sigma_{\mathrm{CP}}(L) = \sigma_{\mathrm{MC}} + (L \times \sigma_{\mathrm{THz}}) \quad (16)$$

Since SE is defined as the achievable capacity per unit of spectrum bandwidth, using (16), the system-level average SE of MNO 1 in bps/Hz can be expressed as follows.

$$\sigma_{\mathrm{SE}}(L) = \sigma_{\mathrm{CP}}(L) / \left((M_{\mathrm{GHz}} + M_{\mathrm{THz}}) \times Q \right) \quad (17)$$

Now, define EE as the amount of energy required to transmit a bit of information, using (16), the system-level EE of MNO 1 in Joule/bit can be expressed as follows.

$$\sigma_{\mathrm{EE}}(L) = \begin{pmatrix} (L \times S_{\mathrm{F}} \times P_{\mathrm{THz,SC}}) + \\ (S_{\mathrm{P}} \times P_{\mathrm{GHz,PC}}) + \\ (S_{\mathrm{M}} \times P_{\mathrm{GHz,MC}}) \end{pmatrix} \Big/ \left(\sigma_{\mathrm{CP}}(L)/Q \right) \quad (18)$$

where S_{M} and S_{P} denote, respectively, the number of macrocells and picocells in the system of MNO 1.

IV. Performance Evaluation and Comparison

Default parameters and assumptions used for the evaluation are given in Table I. Note that due to low output power and high propagation loss, the coverage of THz signals is limited [6]. To overcome these constraints, high-gain antennas at both ends are required. Hence, following [3], we consider horn antennas at the transmitting and receiving ends each with a gain of 21 dB. Assume that $\alpha_{\mathrm{ra,op}} = 0.3$ such that $d_{\mathrm{ra}}^{*} \geq 23.58$ m, which implies that the spectrum can be reused in co-channel small cells that are away from one another by at least three apartments each having a side length of 10 m. This corresponds to an intra-floor cluster size consisting of 9 small cells. Now considering $\alpha_{\mathrm{f}}(d_{\mathrm{er}}) = 55$ dB and $\alpha_{\mathrm{er,op}} = 0.1$, $d_{\mathrm{er}}^{*} \geq 0.089$ m, which implies that the spectrum can be reused on each floor. So, from d_{ra}^{*} and d_{er}^{*}, we can find that a 3D cluster consists of 9 small cells. Hence, for a 6-story building with each floor having 9 apartments, the 140 GHz spectrum can be reused 6 times.

TABLE I. DEFAULT PARAMETERS AND ASSUMPTIONS

Parameters and Assumptions			Value
Cellular layout[2], Inter-Site Distance (ISD)[1,2], transmit direction			Hexagonal grid, dense urban, 3 sectors per macrocell, 1732 m, and downlink
Carrier frequency			2 GHz Non-LOS for MBSs and PBSs, 140 GHz LOS for SBSs
System bandwidth			10 MHz (for 2 GHz), 50 MHz (for 140 GHz)
Number of cells			1 MBS, 2 PBSs, 48 SBSs per building
Transmit power[1] (dBm)			46 for MBS[1], 37 for PBS[1], 10 for SBS[3]
small-scale fading model[1]			Rayleigh for 2 GHz, no small-scale fading effect for 140 GHz
Lognormal shadowing standard deviation (dB)			8 for MBS[2], 10 for PBS[1], and 0.5712 for 140 GHz LOS for SBS[3]
Path loss	MBS and a UE[1]	Indoor macrocell UE	PL(dB)=15.3 + 37.6log$_{10}R$, R is in m
		Outdoor macrocell UE	PL(dB)=15.3 + 37.6log$_{10}R$ + L_{ow}, R is in m
	PBS and a UE[1]		PL(dB)=140.7+36.7log$_{10}R$, R is in km
	SBS and a UE[3]		$PL(\mathrm{dB}) = 75.89 + 21.17 \log_{10}(R)$, R in m
Antenna configuration			Single-input single-output for all BSs and UEs
BS antenna gain			14 dBi for MBS[2], 5 dBi for PBS[1], 21 dB for SBS[3]
UE antenna gain			0 dBi for 2 GHz[2], 21 dB (horn antenna) for 140 GHz[3]
UE noise figure[2]			9 dB (for 2 GHz)[2], 9.56 dB (for 140 GHz)[4]
Total number of macrocell UEs			30
PBS coverage and macrocell UEs offloaded to all PBSs[1], Indoor macrocell UEs[1]			40 m (radius), 2/15, 35%
Scheduler and traffic model[2]			Proportional Fair (PF) and full buffer
Type of SBSs			Closed Subscriber Group (CSG) femtocell BSs
TTI[1] and scheduler time constant (t_c)			1 ms and 100 ms
Total simulation run time			8 ms
Building and small cell models: Number of buildings, floors per building, apartments per floor, small cells per apartment, area of an apartment			L, 6, 8, 1, 10×10 m^2

taken [1]from [7], [2]from [8], [3]from [9], [4]form [10].

Figure 2 shows the SE and EE responses due to reusing 50 GHz spectrum in small cells per building in the 140 GHz band for $\varepsilon = 1$ and $\varepsilon = 6$. Clearly, it can be found that clustering small cells in the 140 GHz band and reusing the same spectrum more than once improve both SE and EE performances. Further, it is expected that the 6G mobile systems will require 10 times average SE [10] (i.e., 270-370 bps/Hz), as well as 10-100 times average EE [11] (i.e., 0.03×10^{-6} to 0.3×10^{-6} Joules/bit), of 5G mobile systems [12]-[13]. Now, from Figure 2, it can be found that the expected average SE and EE can be satisfied by reusing the spectrum to less number of buildings of

 ISBN: 978-1-61208-837-2

small cells (i.e., L=6) than that required (i.e., L=31) when no spectrum reuse is considered.

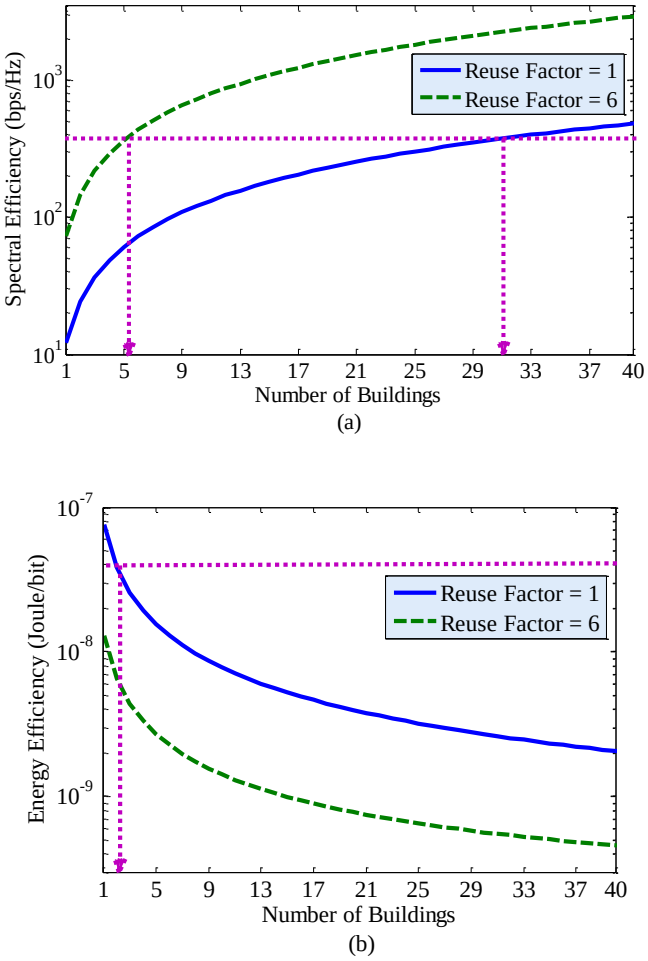


Figure 2. (a) SE and (b) EE responses due to clustering of in-building small cells and reusing the same spectrum $\varepsilon = 6$ times in the 140 GHz band.

V. CONCLUSION

In this paper, we have presented an analytical model to reuse Terahertz (THz) spectrum to small cells of an MNO. All small cells are deployed within buildings and operate only in the 140 GHz band. Interference from one small cell to another due to reusing the 140 GHz spectrum has been modeled both intra-floor and inter-floor levels and the corresponding minimum distance between co-channel small cells have been derived. These minimum distances in the intra-floor and inter-floor level provide the size of a 3D cluster of small cells. We have derived average capacity, Spectral Efficiency (SE), and Energy Efficiency (EE) performance metrics. Extensive simulation and numerical results analyses have been carried out.

It has been found that the 3D clustering of in-building small cells, and reusing the same spectrum in the 140 GHz band to each cluster improve both the SE and EE performances. Moreover, both inter-building reuse factor and intra-building reuse factor have an impact on the overall performance improvement. Finally, we have shown that the presented model can satisfy the prospective SE and EE requirements for the Sixth-Generation (6G) networks by reusing the spectrum in less number of buildings of small cells than that required when no spectrum reuse is considered in the 140 GHz.

REFERENCES

[1] R. K. Saha and C. Aswakul, "A Tractable Analytical Model for Interference Characterization and Minimum Distance Enforcement to Reuse Resources in Three-Dimensional In-Building Dense Small Cell Networks," International Journal of Communication Systems, vol. 30, no. 11, pp. 95-118, July 2017, doi: 10.1002/DAC.3240

[2] R. K. Saha, "Modeling Interference to Reuse Millimeter-Wave Spectrum to In-Building Small Cells Toward 6G," Proc. 2020 IEEE 92nd Vehicular Technology Conference (VTC2020-Fall), Victoria, BC, Canada, 2020, pp. 1-7, doi: 10.1109/VTC2020-Fall49728.2020.9348747.

[3] N. A. Abbasi, A. Hariharan, A. M. Nair, and A. F. Molisch, "Channel Measurements and Path Loss Modeling for Indoor THz Communication," Proc. 2020 14th European Conference on Antennas and Propagation (EuCAP), Copenhagen, Denmark, 2020, pp. 1-5, doi: 10.23919/EuCAP48036.2020.9135643.

[4] R. K. Saha, "3D Spatial Reuse of Multi-Millimeter-Wave Spectra by Ultra-Dense In-Building Small Cells for Spectral and Energy Efficiencies of Future 6G Mobile Networks," Energies, vol. 13, no. 7, Art. no. 1748, 2020, doi: 10.3390/EN13071748

[5] J. Zhao, S. Ni, L. Yang, Z. Zhang, Y. Gong, and X. You, "Multiband Cooperation for 5G Hetnets: A Promising Network Paradigm," IEEE Vehicular Technology Magazine, vol. 14, no. 4, pp. 85-93, Dec. 2019, doi: 10.1109/MVT.2019.2935793.

[6] S. -Y. Zhu, Y. -L. Li, K. -M. Luk, and S. W. Pang, "Compact High-Gain Si-Imprinted THz Antenna for Ultrahigh Speed Wireless Communications," IEEE Transactions on Antennas and Propagation, vol. 68, no. 8, pp. 5945-5954, Aug. 2020, doi: 10.1109/TAP.2020.2986863.

[7] 3GPP *Evolved Universal Terrestrial Radio Access (E-UTRA); Radio Frequency (rf) System Scenarios*: *document 3GPP TR 36.942, V.1.2.0, 3rd Generation Partnership Project, Jul. 2007.* [Online] Available from https://portal.3gpp.org/ desktopmodules /Specifications/Specification Details.aspx?specificationId=2592 (retrieved February 2020)

[8] 3GPP. "*Simulation Assumptions and Parameters for FDD HeNB RF Requirements," document TSG RAN WG4 (Radio) Meeting #51, R4- 092042, 3GPP, May 2009.* [online] Available from: https://www.3gpp.org/ftp/tsg_ran /WG4_Radio/TSGR4_51/Documents/ (retrieved February 2020).

[9] Y. Xing and T. S. Rappaport, "Propagation Measurement System and Approach at 140 GHz-Moving to 6G and Above 100 GHz," Proc. 2018 IEEE Global Communications Conference (GLOBECOM), Abu Dhabi, United Arab Emirates, 2018, pp. 1-6, doi: 10.1109/GLOCOM.2018.8647921.

[10] N. Khalid, N. A. Abbasi and O. B. Akan, "300 GHz Broadband Transceiver Design for Low-THz Band Wireless Communications in Indoor Internet of Things," 2017 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), Exeter, 2017, pp. 770-775, doi: 10.1109/iThings-GreenCom-CPSCom-SmartData.2017.118.

[11] Z. Zhang et al., "6G Wireless Networks: Vision, Requirements, Architecture, and Key Technologies," IEEE Vehicular

 ISBN: 978-1-61208-837-2

Technology Magazine, vol. 14, pp. 28-41, 2019, doi: 10.1109/MVT.2019.2921208.

[12] S. Chen et al., “Vision, Requirements, and Technology Trend of 6G: How to Tackle the Challenges of System Coverage, Capacity, User Data-Rate and Movement Speed,” IEEE Wireless Communications, vol. 27, no. 2, pp. 218-228, April 2020, doi: 10.1109/MWC.001.1900333.

[13] C.-X. Wang et al., “Cellular Architecture and Key Technologies for 5G Wireless Communication Networks,” IEEE Communications Magazine, vol. 52, pp. 122-130, 2014. doi: 10.1109/MCOM.2014.6736752.

[14] G. Auer et al., “How Much Energy is Needed to Run a Wireless Network?,” IEEE Wireless Communications, vol. 18, no. 5, pp. 40-49, October 2011, doi: 10.1109/MWC.2011.6056691.

 ISBN: 978-1-61208-837-2

Performance Analysis of In-building Small Cell Networks: Carrier Frequency Band Perspective

Rony Kumer Saha
Radio and Spectrum Laboratory
KDDI Research, Inc.
2-1-15 Ohara, Fujimino-shi, Saitama, Japan
email: ro-saha@kddi-research.jp

***Abstract*—In this paper, we present the performance of in-building small cells with the variation of carrier frequency from a low microwave band to a very high Terahertz (THz) band expected for the future Sixth-Generation (6G) mobile networks. We derive the average capacity, Spectral Efficiency (SE), Energy Efficiency (EE), and throughput per user of small cell networks. With extensive simulation results, we evaluate these performance metrics with a change in carrier frequency from a microwave band (i.e., 2 GHz), through a number of Millimeter-Wave (mmWave) bands (i.e., 28 GHz and 60 GHz), to a THz band (i.e., 140 GHz). It is shown that due to the presence of Line-of-Sight (LOS) components and availability of large spectrum bandwidth, the high-frequency mmWave and THz bands can play significant roles in improving the above performance metrics and achieve both SE and EE requirements expected for 6G mobile networks by reusing spectrum of their respective bands for a certain number of buildings of small cells.**

***Keywords*—6G; carrier frequency; path loss; in-building; small cell; millimeter-wave, spectrum reuse; THz band.**

I. INTRODUCTION

A. Background

Exponentially increasing mobile traffic and high data rate demands, scarcity of the available radio spectrum, and limitations of the Base Station (BS) transmission power have caused Mobile Network Operators (MNOs) to move from large macrocell-only networks to Heterogeneous Networks (HetNets) [1]. In HetNets, small cells, typically deployed in indoor environments, cover a small area by reusing the spectrum bandwidth and play a significant role in serving high capacity and data rate within a short distance in mobile communication systems. To address the scarcity of available spectrum, the operating spectrum of small cells of one mobile generation shifts toward higher carrier frequencies than that of its predecessor one. As the signal propagation characteristics vary significantly with a change in carrier frequency, the performance of small cells also varies accordingly. This necessitates a deep understanding of how the channel performances within in-building environments vary with a change in the carrier frequency of small cells.

B. Related Work and Problem Statement

Numerous studies addressed the performance evaluation of small cells in multistory buildings, mostly in terms of signal propagation measurements, at different carrier frequencies. For example, the authors in [2] carried out propagation measurements in an indoor building environment at 900 MHz and 450 MHz. In [3], the authors presented a comparative study of two bands, below and above 6 GHz, including 3.5 GHz and 28 GHz. Further, in [4], the authors presented 28 GHz and 73 GHz millimeter-wave (mmWave) propagation measurements performed in a typical office environment. Furthermore, very recently, the authors in [5] performed channel measurements and path loss modeling in the Terahertz (THz) band.

Since the future Sixth-Generation (6G) network is expected to operate in low, as well as very high, frequency bands to address both coverage and capacity demands, instead of a certain frequency band discussed above, a common understanding of how the performance of small cells is affected with a change in the operating carrier frequency (and hence signal propagation characteristics) over a vast range, including very high THz band, is not obvious in the existing studies. To address this concern, in this paper, we present the performance analysis of in-building small cells over a vast range of carrier frequencies, from a low 2 GHz microwave band to a very high 140 GHz band for an efficient utilization of the spectrum in these bands.

In doing so, we consider a range of carrier frequencies that can cover the carrier frequencies of the former, existing, and upcoming mobile generations. More specifically, we start from a microwave band (i.e., 2 GHz used in the former Second-Generation (2G) up to Fourth-Generation (4G)), through a number of mmWave bands (i.e., 28 GHz used in the existing Fifth-Generation (5G) and 60 GHz expected to be used in the enhanced version of the existing 5G), to a THz band (i.e., 140 GHz) proposed to be used in the upcoming 6G mobile networks. However, due to a potential gap from one band to another of the above carrier frequencies, the channel characteristics in one band differ considerably from another. Hence, because of the occurrence of high small-scale fading effects, the Non-Line-of-Sight (NLOS) channel model for the 2 GHz microwave band, whereas the Line-of-Sight (LOS) channel model for the 28 GHz and 60 GHz mmWave bands and the 140 GHz band, are considered and given for a distance d in m in Table I.

C. Contribution

Based on the above discussion and consideration, in this paper, we contribute the following.

- We vary the carrier frequency of small cells from a low 2 GHz band to a very high 140 GHz band and derive the corresponding average capacity, Spectral Efficiency (SE),

 ISBN: 978-1-61208-837-2

Energy Efficiency (EE), and throughput per in-building small cell user performance metrics.

TABLE I. CHANNEL MODELS FOR DIFFERENT CARRIER FREQUENCY BANDS.

Channel Model		Value
Path loss Carrier Frequency	2 GHz[1,2]	$127+30\log_{10}(d/1000)$
	28 GHz[5]	$61.38+17.97\log_{10}(d)$
	60 GHz[3]	$68+21.7\log_{10}(d)$
	140 GHz[4]	$75.89+21.17\log_{10}(d)$
Lognormal Shadowing standard deviation (dB)		10 (for 2 GHz)[1,2], 9.9 (for 28 GHz)[5], 0.88 (for 60 GHz)[3], and 0.5712 (for 140 GHz)[4]
Small-scale fading model		Frequency selective Rayleigh for 2 GHz[1], no small-scale fading effect for 28 GHz[5], 60 GHz[3], and 140 GHz[4]

taken [1]from [6], [2]from [7], [3]from [8], [4]from [5], [5]from [9].

- We carry out extensive simulation results and evaluate these performance metrics to show the significance of the variation in the operating carrier frequency on the performance of in-building small cell networks.
- Finally, we present a performance comparison against both SE and EE requirements expected for the 6G mobile networks by reusing the spectrum of each carrier frequency band for a certain number of buildings of small cells.

D. Organization

The paper is organized as follows. In Section II, we discuss the system architecture to evaluate the performance and derive performance metrics in terms of average capacity, Spectral Efficiency (SE), Energy Efficiency (EE), as well as average throughput per small cell user for all carrier frequencies. In Section III, performance evaluation scenarios are described, and extensive simulation results and performance comparisons are carried out. We draw a conclusion in Section IV.

II. System Architecture and Performance Metrics

A. System Architecture

We consider a simple system architecture for the performance evaluation as shown in Figure 1. A number of Picocell Base Stations (PBSs) are located outdoors, and all small cell BSs (SBSs) are located indoors within a number of buildings situated over the coverage of a Microcell Base Station (MBS). A number of Macrocell User Equipments (UEs) are considered indoors and all other outdoor Macrocell UEs (MUEs) are either served by the MBS or offloaded to nearby PBSs. However, all Small Cell UEs (SUEs) are served only by in-building SBSs. Both MBSs and PBSs operate in the 2 GHz band, whereas all SBSs operate at either 2 GHz, 28 GHz, 60 GHz, or 140 GHz band at any time.

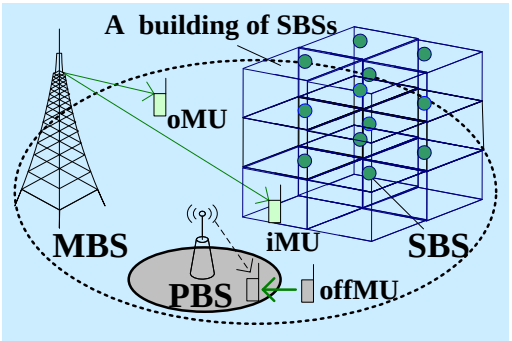


Figure 1. System architecture. oMU, iMU, and offMU define outdoor, indoor, and offloaded MUEs, respectively.

B. Performance Metrics Estimation

1) Preliminary: Let M_2, M_{28}, M_{60}, and M_{140} denote, respectively, the number of Resource Blocks (RBs) in the 2 GHz, 28 GHz, 60 GHz, and 140 GHz bands where an RB is equal to 180 kHz. Let M_{MC} denote the number of RBs in the 2 GHz band allocated exclusively to MBSs and PBSs, and hence is orthogonal to M_2 to avoid Co-Channel Interference (CCI) with SUEs. Let $P_{t,i}$, $N_{t,i}$, and $I_{t,i}$ denote, respectively, the transmission power, noise power, and total interference signal power at any RB *i* in Transmission Time Interval (TTI) *t*.

Using the formulas given in Table I, the path loss can be calculated for each carrier frequency. Let $PL_{t,i}$, $LS_{t,i}$, and $SS_{t,i}$ denote, respectively, the path loss, large-scale shadowing, small-scale fading between a SBS and an SUE at RB *i* in TTI *t*. Let (G_t+G_r) and L_F denote, respectively, the total antenna gain and connector loss such that a link channel response, denoted as $H_{t,i}$, between an SUE and a SBS at RB *i* in TTI *t* can be given by in dB as follows.

$$H_{t,i}(\text{dB}) = (G_t+G_r)-(L_F+PL_{t,i})+(LS_{t,i}+SS_{t,i}) \quad (1)$$

The received Signal-to-Interference-plus-Noise Ratio (SINR) for an SUE at RB *i* in TTI *t* can be expressed as follows.

$$\rho_{t,i} = \left(P_{t,i}/(N_{t,i}+I_{t,i})\right).H_{t,i} \quad (2)$$

Using Shannon's capacity formula, a link throughput at RB *i* in TTI *t* in bps per Hz is given by,

$$\sigma_{t,i}(\rho_{t,i}) = \begin{cases} 0, & \rho_{t,i} < -10\,\text{dB} \\ \beta\log_2\left(1+10^{(\rho_{t,i}(\text{dB})/10)}\right), & -10\,\text{dB} \le \rho_{t,i} \le 22\,\text{dB} \\ 4.4, & \rho_{t,i} > 22\,\text{dB} \end{cases} \quad (3)$$

where β denotes implementation loss factor.

The total capacity of all MUEs in $t \in \boldsymbol{T}=\{1,2,\ldots,Q\}$ is given by,

$$\sigma_{\text{MU}} = \sum_{t=1}^{Q}\sum_{i=1}^{M_{\text{MC}}}\sigma_{t,i}(\rho_{t,i}) \quad (4)$$

Now, the aggregate capacity served by a SBS in a building in $t \in \boldsymbol{T}$ over M_2 RBs is given by,

$$\sigma_s = \sum_{t\in\boldsymbol{T}}\sum_{i=1}^{M_2}\sigma_{t,i}(\rho_{t,i}) \quad (5)$$

Let S_F denote the number of SBSs per building. The aggregate capacity served by all SBSs in a single building when operating only in the 2 GHz band is then given by,

$$\sigma_{SU,2,L=1} = \sum_{s=1}^{S_F} \sigma_s \quad (6)$$

$$\sigma_{SU,2,L=1} = \sum_{s=1}^{S_F} \sum_{t \in \mathcal{T}} \sum_{i=1}^{M_2} \sigma_{t,i} \left(\rho_{t,i} \right) \quad (7)$$

2) Average capacity, SE, and EE: Let P_2, P_{28}, P_{60}, and P_{140} denote, respectively, the transmission power of a small cell when operating in the 2 GHz, 28 GHz, 60 GHz, and 140 GHz bands. P_M and P_P denote, respectively, the transmission power of an MBS and a PBS. Let S_M, S_P, and S_F denote, respectively the number of MBSs, PBSs, and SBSs per building. Because of the small coverage and low transmission power of a SBS, as well as low SUE speed, an indoor channel does not vary considerably within a short time such that we consider similar indoor signal propagation characteristics for all L buildings per macrocell.

Then, by linear approximation, the system-level average capacity per macrocell of the MNO is given by the sum of the aggregate capacity of all macrocell UEs and the aggregate capacity of all small cell UEs in L buildings. So, using (4) and (7), the system-level average capacity per macrocell is given by

$$\sigma_{2,L>1} = \sigma_{MU} + \left(L \times \sigma_{SU,2,L=1} \right) \quad (8)$$

Since SE is defined as the achievable capacity per unit of spectrum bandwidth, using (8), the system-level average SE in bps/Hz can be expressed as follows.

$$\gamma_{2,L>1} = \sigma_{2,L>1} \Big/ \left(\left(M_{MC} + M_2 \right) \times Q \right) \quad (9)$$

Since EE can be defined as the amount of energy required to transmit a bit of information, using (8), the system-level EE in Joule/bit can be expressed as follows.

$$\varepsilon_{2,L>1} = \left(\begin{matrix} \left(L \times S_F \times P_2 \right) + \\ \left(S_M \times P_M + S_P \times P_P \right) \end{matrix} \right) \Big/ \left(\sigma_{2,L>1} / Q \right) \quad (10)$$

3) Average throughput per SUE: Assume that each SBS can serve one SUE at any time in all carrier frequencies. The average throughput per SUE when SBSs operate in the 2 GHz band can then be expressed for S_F SBSs per building as follows.

$$\sigma_{2,s} = \sigma_{SU,2,L=1} / S_F \quad (11)$$

Following the above procedure and using (4)-(9) for the 2 GHz band, the system-level average capacity, SE, EE, and average throughput per SUE when small cells operate in the 28 GHz, 60 GHz, and 140 GHz can also be derived.

III. Performance Evaluation Scenario, Result, and Comparison

A. Performance Evaluation Scenario

Default simulation parameters and assumptions for SBSs are given in Table II. For MBSs and PBSs, detailed parameters and assumptions can be found in [10]. Note that, for fair analysis, we consider the same parameters and assumptions, wherever applicable, including system bandwidth, symbol duration, transmission power, antenna configuration, and antenna gain of all SBSs and UEs, for all carrier frequencies even though they differ from one carrier frequency to another in practice. RBs of any band are allocated orthogonally to SBSs in any TTI by the Proportional Fair (PF) scheduler to avoid CCI between SBSs. Moreover, for simplicity, we assume that no CCI effect is experienced by any in-building SBS when operating in the 60 GHz band due to coexisting with the IEEE 802.11ad/ay, also termed as Wireless Gigabit (WiGig), access points.

Further, we assume that each MNO in a country is allocated to a dedicated spectrum in the 2 GHz, 28 GHz, and 140 GHz bands such that no CCI effect is experienced by any in-building SBS due to operating in the spectrum by SBSs of another MNO. Such CCI can be either avoided using techniques such as the time-domain Almost Blank Subframe based Enhanced Intercell Interference Coordination (eICIC) technique for Long Term Evolution (LTE) systems or mitigated using techniques such as the underlay cognitive radio spectrum access technique, which we consider out of the scope of this paper. Finally, we generate the performance results by simulating all assumptions and parameters given in Tables I and II by a simulator built using the computational tool MATLAB R2012b version running on a personal computer.

TABLE II. DEFAULT PARAMETERS AND ASSUMPTIONS

Parameters and Assumptions	Value
Transmit direction	Downlink
SBS operating bandwidth	50 MHz (for each carrier frequency)
Number of RBs in the SBS bandwidth	250 (for each carrier frequency)
Number of SBSs	48 (per building)
Transmission power (dBm)[7]	10 (for each carrier frequency)
Antenna configuration	Single-input single-output for all SBSs and SUEs
SBS antenna gain[7]	21 dB
SUE antenna gain[7] and noise figure	21 dB and 10 dB
Scheduler and traffic model[6]	Proportional Fair (PF) and full buffer
Type of SBSs	Closed Subscriber Group (CSG) femtocell BSs
Building and small cell models:	
Number of buildings, floors per building,	L, 6,
apartments per floor, small cells per apartment,	8, 1,
area of an apartment	10×10 m^2
TTI[8] and scheduler time constant (t_c)	1 ms and 100 ms
Total simulation run time	8 ms

taken from [6]from [7], [7]from [5], [8]from [6].

B. Performance Evaluation Result

Figure 2(a) shows the path loss response for a SBS with the variation in distance d of its SUE. It can be found that the path loss at distance d from a SBS is the most when the SBS operates in the 140 GHz band, and the least, when it operates in the 2 GHz microwave band. In general, with an increase in the carrier frequency, the path loss increases since a high-frequency signal gets affected more by the propagating environment than that of a low-frequency one. This implies that to address high capacity and data rate demands of the future mobile networks, the

availability of large spectrum bandwidth in the high-frequency bands such as THz bands will play a vital role in serving high capacity and data rate demands within a short indoor distance from a SBS.

Figure 2(b) shows the response of the average throughput per SUE in different carrier frequencies. It can be observed that, for LOS signal propagations in the high-frequency bands, the average throughput per SUE over a certain time *T* decreases with an increase in the carrier frequency. This is because an increase in carrier frequency causes to increase in the distant-dependent path loss as shown in Figure 2(a). However, the average throughput per SUE is the lowest when SBSs operate in the 2 GHz low-frequency band. This is due to the NLOS signal propagation that occurs from the presence of large multipath fading components in the low-frequency band unlike the high-frequency one with a LOS signal propagation as aforementioned.

Figures 3(a) and 3(b) show, respectively, the system-level SE and EE performances for the 10 MHz bandwidth of all MUEs. Recall that due to considering the LOS models, high-frequency signals offer high average capacity, as well as average throughput per SUE because of highly directive signal propagation toward SUEs such that by forming appropriate beam width, the enormous amount of average capacity and hence SE can be obtained. Moreover, due to an increase in average capacity, the average energy required per bit transmission is also reduced, resulting in improving EE as well.

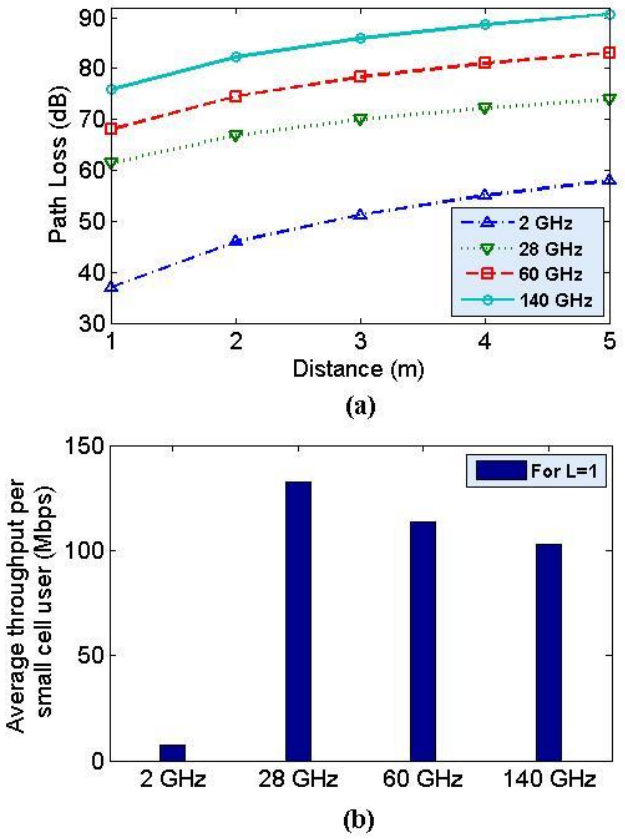


Figure 2. (a) Path loss and (b) average throughput per SUE responses with a variation in the carrier frequency of in-building SBSs.

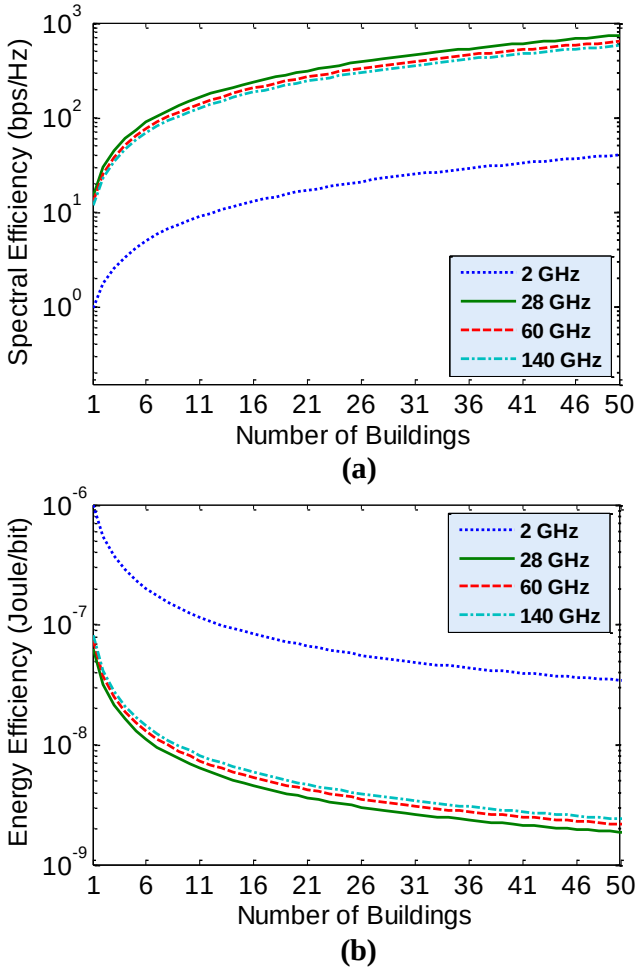


Figure 3. System-level performances with a variation in the carrier frequency of in-building SBSs. (a) spectral efficiency and (b) energy efficiency.

From Figure 2(a), since the path loss increases with an increase in LOS carrier frequency, the system-level SE and EE improve with a decrease in carrier frequency. Hence, the maximum and minimum improvements in both SE and EE are obtained when SBSs operate in the 28 GHz and 140 GHz bands, respectively. However, due to the NLOS signal propagation effect, the 2 GHz band provides the worst performance in the average capacity (Figure 2(b)), resulting in realizing the worst system-level SE and EE performances in NLOS 2 GHz carrier frequency as shown in Figures 3(a) and 3(b).

C. Performance Evaluation Comparison

Recall that unlike the low-frequency 2 GHz microwave band, which is affected considerably by the multipath fading effect from the reflection, refraction, and scattering phenomenon, due to the presence of LOS components and availability of large spectrum bandwidth, high carrier frequency bands can play significant roles in improving the in-building average throughput per SUE, as well as system-level average capacity, SE, and EE of the future mobile systems.

In this regard, assume that the prospective average SE and EE requirements for 6G mobile networks are, respectively, 10

 ISBN: 978-1-61208-837-2

times (i.e., 370 bps/Hz) [11] and 10-100 times (i.e., 0.3μJ/bit - 0.03μJ/bit) [12] higher than that of 5G mobile networks [13]-[14]. From Figures 3(a) and 3(b), it can be found that all high carrier frequency bands, i.e., 28 GHz, 60 GHz, and 140 GHz, can achieve both SE and EE requirements expected for 6G mobile networks by reusing spectrum in their respective bands for a reuse factor (i.e., *L*) of 26, 30, and 33, respectively.

IV. CONCLUSION

Small cells deployed in indoor environments play a significant role in serving high capacity and data rate within a short distance in mobile communication systems. Due to the scarcity of spectrum, the operating spectrum of small cells of one mobile generation shifts toward higher carrier frequencies than that of its predecessor one. As the signal propagation characteristics vary significantly with a change in carrier frequency, in this paper, we have presented the performance of in-building small cells with the variation of carrier frequency from a low microwave band to a very high Terahertz (THz) band expected for the future Sixth-Generation (6G) mobile networks.

We have derived the average capacity, Spectral Efficiency (SE), Energy Efficiency (EE), and throughput per small cell UE (SUE) and carried out extensive simulation results with a change in carrier frequency from a microwave band (i.e., 2 GHz), through a number of millimeter-wave (mmWave) bands (i.e., 28 GHz and 60 GHz), to a THz band (i.e., 140 GHz). It has been shown that due to the presence of LOS components, high-frequency signals offer high average capacity and hence SE, as well as average throughput per SUE. Moreover, due to an increase in average capacity, the average energy required per bit transmission is also reduced, resulting in improving EE as well. Since the path loss increases with an increase in LOS carrier frequency, the maximum and minimum improvements in both SE and EE are obtained when SBSs operate in the 28 GHz and 140 GHz bands, respectively.

However, due to the NLOS signal propagation effect, the 2 GHz band is affected considerably by the multipath fading effect from the reflection, refraction, and scattering phenomenon such that the 2 GHz band provides the worst performance in the average capacity. This results in achieving the worst system-level SE and EE performances. Finally, it has been shown that all high carrier frequency bands, i.e., 28 GHz, 60 GHz, and 140 GHz, can achieve both SE and EE requirements expected for 6G mobile networks by reusing spectrum in their respective bands for a reuse factor (i.e., *L*) of 26, 30, and 33, respectively.

REFERENCES

[1] D. López-Pérez, M. Ding, H. Claussen, and A. H. Jafari, "Towards 1 Gbps/UE in Cellular Systems: Understanding Ultra-Dense Small Cell Deployments," IEEE Communications Surveys & Tutorials, vol. 17, no. 4, pp. 2078-2101, Fourthquarter 2015, doi: 10.1109/COMST.2015.2439636.

[2] A. Chandra, "Comparative Study of 900 MHz and 450 MHz Radio Signals Propagation in an Indoor Environment," Proc. 1996 IEEE International Conference on Personal Wireless Communications Proceedings and Exhibition. Future Access, New Delhi, India, 1996, pp. 247-253, doi: 10.1109/ICPWC.1996.494278.

[3] A. M. Al-Samman et al., "Comparative Study of Indoor Propagation Model Below and Above 6 GHz for 5G Wireless Networks. Electronics, vol 8, no. 44, 2019. doi:10.3390/electronics8010044

[4] S. Deng, M. K. Samimi, and T. S. Rappaport, '28 GHz and 73 GHz millimeter-wave Indoor Propagation Measurements and Path Loss Models," Proc. 2015 IEEE International Conference on Communication Workshop (ICCW), London, UK, 2015, pp. 1244-1250, doi: 10.1109/ICCW.2015.7247348.

[5] N. A. Abbasi, A. Hariharan, A. M. Nair, and A. F. Molisch, "Channel Measurements and Path Loss Modeling for Indoor THz Communication," Proc. 2020 14th European Conference on Antennas and Propagation (EuCAP), Copenhagen, Denmark, 2020, pp. 1-5, doi: 10.23919/EuCAP48036.2020.9135643.

[6] 3GPP. *Evolved Universal Terrestrial Radio Access (E-UTRA); Radio Frequency (RF) System Scenarios. Document 3GPP TR 36.942, V.1.2.0, 3rd Generation Partnership Project, Jul. 2007*. [online] Available from: https://portal.3gpp.org/ desktopmodules /Specifications/Specification Details.aspx?specificationId=2592 [retrieved February, 2020]

[7] *Simulation Assumptions and Parameters for FDD HeNB RF Requirements. document TSG RAN WG4 (Radio) Meeting #51, R4-092042, 3GPP, May 2009*. [online] Available from: https://www.3gpp.org/ftp/tsg_ran /WG4_Radio/TSGR4_51 /Documents/ [retrieved February, 2020].

[8] S. Geng, J. Kivinen, X. Zhao, and P. Vainikainen, "Millimeter-Wave Propagation Channel Characterization for Short-Range Wireless Communications," IEEE Transactions on Vehicular Technology, vol. 58, no. 1, pp. 3-13, Jan. 2009, doi: 10.1109/TVT.2008.924990.

[9] G. R. Maccartney, T. S. Rappaport, S. Sun, and S. Deng, "Indoor Office Wideband Millimeter-Wave Propagation Measurements and Channel Models at 28 and 73 GHz for Ultra-Dense 5G Wireless Networks," IEEE Access, vol. 3, pp. 2388-2424, 2015, doi: 10.1109/ACCESS.2015.2486778

[10] R. K. Saha, "3D Spatial Reuse of Multi-Millimeter-Wave Spectra by Ultra-Dense In-Building Small Cells for Spectral and Energy Efficiencies of Future 6G Mobile Networks," Energies, vol. 13, no. 7, 1748, pp.1-19, 2020. doi: 10.3390/EN13071748

[11] Z. Zhang et al., "6G Wireless Networks: Vision, Requirements, Architecture, and Key Technologies," IEEE Vehicular Technology Magazine, vol. 14, no. 3, pp. 28-41, Sept. 2019, doi: 10.1109/MVT.2019.2921208.

[12] S. Chen et al. , "Vision, Requirements, and Technology Trend of 6G: How to Tackle the Challenges of System Coverage, Capacity, User Data-Rate and Movement Speed," IEEE Wireless Communications, vol. 27, no. 2, pp. 218-228, April 2020, doi: 10.1109/MWC.001.1900333.

[13] C. Wang et al., "Cellular architecture and Key Technologies for 5G Wireless Communication Networks," IEEE Communications Magazine, vol. 52, no. 2, pp. 122-130, February 2014, doi: 10.1109/MCOM.2014.6736752.

[14] G. Auer et al., "How much energy is needed to run a wireless network?," IEEE Wireless Communications, vol. 18, no. 5, pp. 40-49, October 2011, doi: 10.1109/MWC.2011.6056691.

 ISBN: 978-1-61208-837-2

Containerization Using Docker Technology

Alexandru Eftimie
University POLITEHNICA of Bucharest, Bucharest, Romania
Department of Telecommunication, University "Politehnica" of Bucharest, Romania
E-mail: alexandru.eftimie@gmail.com

Eugen Borcoci
University POLITEHNICA of Bucharest, Bucharest, Romania
Department of Telecommunication, University "Politehnica" of Bucharest, Romania
E-mail: eugen.borcoci@elcom.pub.ro

***Abstract*— This paper aims to provide a clearer view of container technology, such as its advantages and disadvantages, how it can cooperate with Openstack, and document the improvements made by this cooperation. In terms of containerization technology, this paper will illustrate the components of Docker and the impact it has compared to the already classic technology of virtual machines. Another element to be addressed in this paper is the importance of moving some of the computing power to the periphery of networks. This can be done using existing peripheral devices to the extent that the computing resources on this equipment allow. This move is necessary to provide an infrastructure capable of supporting services with low latency needs, minimal delay (traffic sensor, vehicle sensors) and at the same time an infrastructure that will free the core of networks from a large volume of data. This paper will follow the comparison of household equipment that can play an active role in computing at the periphery of networks to highlight what types of applications or calculations can be performed on them. We will follow in this paper the comparison of household equipment that can play an active role in computing at the periphery of networks to highlight what types of applications or calculations can be performed on them.**

Keywords-container; Docker; Network Function Virtualization (NFV).

I. INTRODUCTION

Currently, typical network architectures have three main areas: access, transport, and core. Most of computational resources for applications are in the cloud, far away from the end user. Another element which will be addressed in this paper is the importance of moving some of the computing power to the periphery of networks. This can be done using existing peripheral devices, like routers, dedicated gateways, servers, to the extent that the computing resources on this equipment allow [1]. This move is necessary to provide an infrastructure capable of supporting services with low latency needs, minimal delay and at the same time an infrastructure that will free the core of networks from a large volume of data. We will follow in this paper the comparison of household equipment that can play an active role in computing at the periphery of networks to highlight what types of applications or calculations can be performed on them.

Recently, we have seen a trend called "fog computing" (an architecture that uses edge devices to carry out a substantial amount of computation) and, therefore, the need for processing on the periphery of networks. Hence, there is a need to implement computing and processing machines in this area, a need we have not encountered so far. Given that the services that are liable to be moved to the edge of the network ("edge computing") are diverse and offered by various providers, a possible solution could be the implementation of OpenStack on the periphery of networks by Internet providers / transport providers.

In Section 2 an overview of the containerization technology is going to be described, illustrating the advantages it has compared with virtual machines. Section 3 will cover the Docker technology illustrating its components, the architecture and how the isolation is achieved. In Section 4 we will describe the cooperation between Network Function Virtualization (NFV) and containers and compare current approaches and platforms used to migrate computational resources to the edge of the network.

II. CONTAINERS AND MICROSERVICES

Containerization [2] has become a major trend in software development as an alternative or companion to virtualization [3]. This involves encapsulating or packaging the software code and all its dependencies so that it can run smoothly and consistently on any infrastructure. The technology has matured rapidly, leading to measurable benefits for developers and operations teams, as well as general software infrastructure.

Containerization allows developers to create and deploy applications faster and more securely. With traditional methods, the code is developed in a specific computing environment which, when transferred to a new location, often leads to bugs and errors.

Containers are often referred to as "lightweight", which means that they share the core of the machine's Operating System (OS) and do not require the association of an operating system within each application. Containers are inherently smaller than a virtual machine and require less

 ISBN: 978-1-61208-837-2

start-up time, allowing many more containers to run on the same computing power as a single Virtual Machine (VM). This leads to higher server efficiencies and, in turn, reduces server and licensing costs.

Simple containerization allows applications to be "written once and run anywhere." This portability is important in terms of the development process and supplier compatibility. It also offers other notable advantages, such as fault isolation and ease of management and security [4].

Containerization offers significant benefits to developers and development teams. These include the following:

- Portability: A container creates an executable software package that is abstracted (unattached or unattended) from the host operating system and, therefore, portable and able to run smoothly and consistently on any platform or cloud.
- Agility: The open source Docker engine for running containers has started the industry standard for containers with simple tools for developers and a universal presentation approach that works on both Linux and Windows operating systems. The container ecosystem has shifted to engines managed by the Open Container (OCI) initiative.
- Speed: Containers are often referred to as “lightweight,” which means they share the core of the machine’s OS. Not only does this lead to higher server efficiency, but it also reduces server and licensing costs, while speeding up startup times because there is no operating system to boot.
- Defect isolation: Each containerized application is isolated and operates independently of the others. The failure of one container does not affect the continuous operation of other containers. Development teams can identify and correct any technical issues in one container without having to consider other containers.
- Efficiency: Software running in containerized environments shares the machine's operating core and application layers in a container can be shared across containers. Thus, the containers are inherently smaller than a VM and require less start-up time, allowing many more containers to run on the same computing power as a single VM.
- Easy to manage: A container orchestration platform automates the installation, scaling and management of containerized tasks and services. Container orchestration platforms can make management tasks easier, such as scaling containerized applications, running newer versions of applications, and providing monitoring, recording, and debugging, among other functions.

Software companies, large and small, accept microservices as a superior approach to application development and management, compared to the previous monolithic model that combines a software application with the associated user interface and the underlying database in a single unit on a single server platform. With the help of microservices, a complex application is divided into a series of smaller, more specialized services, each with its own database and its own business logic. Microservices then communicate with each other through common interfaces (such as APIs) and REST interfaces (such as HTTP). Using microservices, development teams can focus on updating certain areas of an application without impacting it, leading to faster development, testing, and implementation.

Containers, microservices and cloud computing work together to bring application development and delivery to new levels, which are not possible with traditional methodologies and environments. These next-generation approaches add agility, efficiency, reliability, and security to the software development lifecycle - all leading to faster application delivery and improvements to end users and the marketplace [4].

III. DOCKER

Docker is an open platform for developing, transporting, and running applications. Docker allows applications to be separated from the infrastructure so that software can be delivered quickly. With Docker, the infrastructure can be managed the same way the applications are managed. By taking advantage of Docker's methodologies for fast code forwarding, testing, and implementation, the delay between writing code and running it in production can be significantly reduced.

Docker offers the ability to wrap and run an application in an isolated environment called a container. Isolation and security allow multiple containers to run simultaneously on a given host. Containers are light because they do not need to be overloaded by a hypervisor, but run directly into the core of the host machine. This means that more containers can be run on a given hardware combination than if virtual machines are used. One can even run Docker containers in host machines that are virtual machines.

Docker provides tools and a platform to manage the container lifecycle:

- The application and its support components can be developed using containers.
- The container becomes the unit for distributing and testing the application.
- Implementing the application in the production environment, as a container or an orchestrated service. This works the same whether the production environment is a local data center, a cloud provider, or a hybrid of the two.

Docker Engine is a client-server application with the following major components, depicted also in Figure 1:

- A server that is a type of long-term program called a daemon process.
- REST API that specifies the interfaces that programs can use to talk to the daemon and instruct it on what to do.
- A Command Line Interface (CLI) client.

 ISBN: 978-1-61208-837-2

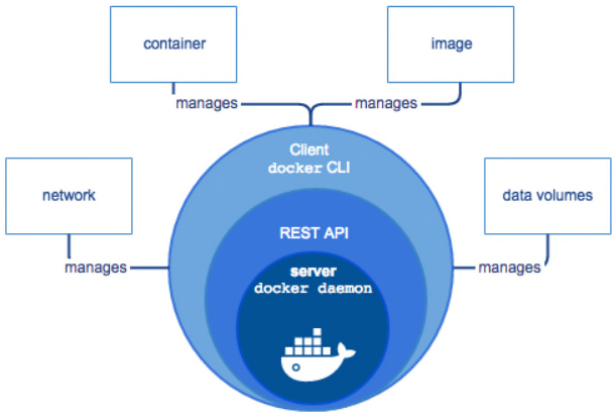


Figure 1. Docker components [5]

The Docker container-based platform enables portable workloads. Docker containers can run on the developer's local laptop, on physical or virtual machines in a data center, on cloud providers, or in a hybrid environment. Docker's portability and lightweight nature make it easy to dynamically manage workloads, extend or eliminate applications and services, as required, in real time.

A. Docker arhitecture

Docker uses a client-server architecture. As illustrated in Figure 2, the Docker client speaks to the Docker daemon, which makes it difficult to lift the construction, run, and distribute Docker containers. The Docker client and daemon can run on the same system, or a Docker client can connect to a remote Docker daemon. The Demon client and daemon communicate using a REST API, through UNIX sockets, or a network interface.

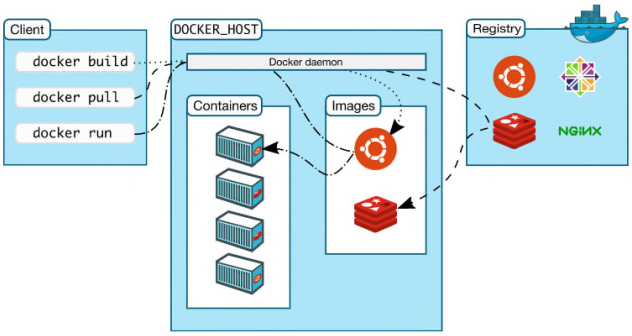


Figure 2. Docker architecture [5]

An image is a read-only template with instructions for creating a Docker container. Often, one image is based on another image, with some additional customizations. For example, one can build an image that is based on the ubuntu image, but installs the Apache web server and application, as well as the configuration details needed to run the application.

One can create new images or use only those created by others and published in a register. To build a new image, a Docker file is created with a simple syntax to define the necessary steps to create the image and run it. Each statement in a Docker file creates a layer in the image. When the Docker file is changed and the image is rebuilt, only those modified layers are rebuilt. This is part of what makes images so light, small and fast compared to other virtualization technologies.

A container is an executable instance. One can create, start, stop, move, or delete a container using the Docker API or CLI and it is possible to connect a container to one or more networks, attach its storage, or even create a new image based on its current state [5].

B. Isolation in Docker technology

Docker isolates different containers by combining four main concepts:

- Groups.
- Namespaces.
- Stackable image layers and copy writing.
- Virtual network bridges.

Control groups are a way of assigning a subset of resources to a particular process group. This can be common, for example, if we make sure that even if the processor is very busy with Python scripts, the PostgreSQL database still receives dedicated CPU and RAM. Figure 3 illustrates this in an example scenario with 4 processor cores and 16 GB RAM:

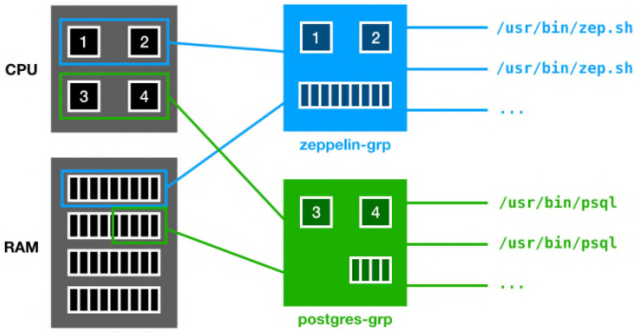


Figure 3. Allocation of resources to control groups [6]

Figure 4 illustrates the parts of a typical process tree in which the init process started a logging service (syslogd), a scheduler (cron), and a connection shell (bash). Within this tree, each process can see all other processes and can send signals (for example to request that the process be stopped) if desired. Using PID namespaces virtualizes the PIDs for a specific process and all of its subprocesses, leading it to believe that it has PID 1. It will also not be able to see any process other than its own children.

```
1
/sbin/init
          +-- 196 /usr/sbin/syslogd -s
          +-- 354 /usr/sbin/cron -s
          +-- 391 login
              +-- 400 bash
                  +-- 701 /usr/local/bin/pstree
```

Figure 4. Process tree [6]

 ISBN: 978-1-61208-837-2

To achieve file system isolation, the namespace will map a node from the file system tree to a virtual root inside that name. By searching for the file system in that namespace, Linux will not allow user to go beyond the virtualized root. Figure 5 shows a part of a file system that contains several roots of the "virtual" file system in the / drives / xx folders, each containing different data.

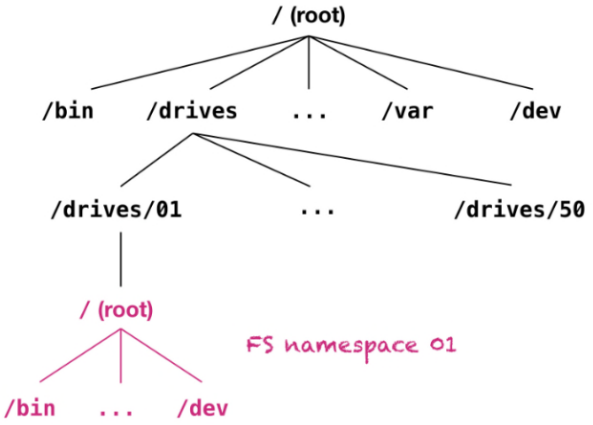


Figure 5. Part of a file system that contains multiple "virtual" file system roots [6]

Docker has a persistence of images in stackable layers. A layer contains changes to the previous level. For example, if one installs Python first and then copy a Python script, the image will have two additional layers: one that contains Python executables and one that contains the script. In Figure 6 a Zeppelin, a Spring and a PHP image are showed.

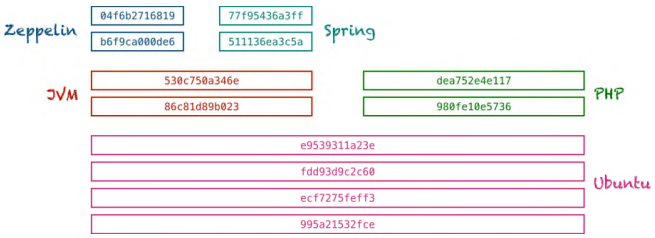


Figure 6. Ubuntu-based Zeppelin, Spring and PHP images [6]

In order not to store Ubuntu three times, the layers are immutable and shared. Docker uses copy-on-write to make a copy of a file only if there are changes. When an image-based container is started, the Docker daemon will provide all the layers contained in that image and place it in an isolated file system namespace for that container. The combination of stackable layers, copy-on-write namespaces, and file system allows a container to run completely independent of things "installed" on the Docker host without wasting much space. This is one of the reasons why containers are lighter compared to virtual machines.

IV. CONTAINERS IN NFV

To cope with the growing use of networks, driven by new mobile customers, and to meet the demand for new network services and performance guarantees, telecom service providers leverage virtualization on their network by implementing network services in virtual machines. They are disconnected from traditional hardware. This effort, known as NFV, reduces operating expenses and offers new business opportunities. At the same time, new mobile networks, new enterprise and IoT networks introduce the concept of "computing capabilities" that are pushed to the edge of the network, in the immediate vicinity of users. However, the strong footprint of current NFV platforms prevents them from operating at the edge of the network [6].

Data consumption is growing exponentially in today's communications networks. This irreversible trend is determined by the increase in the number of end users and the widespread penetration of new mobile devices (smartphones, portable devices, sensors, etc.). In addition, the consumption of mobile data is also accelerated by the increased capabilities of mobile customers (e.g., higher-resolution screens and HD cameras) and the user's desire for high-speed, always-on, multimedia-oriented connectivity. At the same time, the Telecommunications Service Provider (TSP) market is becoming competitive as the number of “on top” service providers increase, reducing user subscription fees.

As a result, telecom service providers have begun to lose existing revenue, while suffering increased capital expenditures and operating costs that cannot be offset by rising subscription costs. To meet the challenges mentioned above, service providers have begun to migrate network infrastructure to software. By virtualizing traditional services providers can save operational and capital costs and meet user requirements for personalized services. This transformation, called network virtualization, is transforming the way operators build their network architecture to disconnect network functionality from physical locations for faster and more flexible network provisioning.

In Table 1, some popular marginal devices are presented along with their release date, architecture, CPU, and memory parameters. The list includes residential equipment for large-scale customers. As can be seen from Table 1, recent CPE devices and home routers are equipped with powerful computing capabilities (e.g., processors up to 1.6 GHz) and a considerable amount of RAM (up to 1 GB) for run a Linux-based operating system (OpenWRT or DD-WRT).

TABLE I. EDGE DEVICES SPECIFICATION [2]

Customer Device	Architecture	CPU	Memory
Residential CPE home routers			
Virgin SuperHub 3(Arris TG2492s)	Intel Atom	2x1.4 GHz	2x256 MB
Google Fiber Network Box GFRG110	ARM v5	1.6 GHz	N/A
Orange Livebox 4	Cortex A9	1 GHz	1 GB
Commodity wireless routers			
TP-LINK Archer C9 home router	ARM v7	2x1 GHz	128 MB
Ubiquity Edge Router Lite 3	Cavium MIPS	2500 MHz	512 MB
Netgear R7500 Smart Wifi Router	Qualcomm Atheros	2x1.4 GHz	384 MB
IoT edge gateways			
Dell Edge Gateway 5000	Intel Atom	1.33 GHz	2 GB

NEXCOM CPS 200 Industrial IoT Edge Gateway	Intel Celeron	4x2.0 GHz	4 GB
HPE Edgeline EL4000	Intel Xeon	4x3.0 GHz	Up to 64 GB

As demonstrated in "Container Network Functions" [2], even a home TP-Link router with a 560 MHz processor and 128 MB of RAM can be used to run multiple VNFs using Linux containers. In addition to low-cost marginal devices, such as home routers and residential Customer Premises Equipments (CPE), some vendors have also introduced IoT gateways with state-of-the-art processors and up to 64 GB of RAM to host new services, such as intelligent analysis at the edge of the network.

While positioning at the edge of the network has many advantages, traditional NFV platforms have been built on high-power servers, mainly operating virtual machines (using technologies, such as Xen Project [7] or Kernel Virtual Machine [8]) for VNF. Table 2 summarizes the features supported by some existing solutions. The information presented reflects the public information available at the time of writing. Cloud4NFV [1] is a platform that promises to provide a new service to end customers, based on cloud, defined software networks and WAN technologies. The research projects UNIFY [3] and T-NOVA [7] share a similar vision of the unification of cloud networks and providers by implementing a system of "network functions as a service". The OPNFV Linux project is the most popular open source NFV platform, with support and implementations from many vendors and large vendors. While all these platforms have made important contributions in the field, none of them has so far featured a container-based, network-focused and mobility-focused NFV system.

TABLE 1. SUMMARY OF EXISTING APPROACHES [2]

	GNF	Cloud NFV [1]	UNIFY	T-NOVA [7]	OPNFV
Virtualization technology	Container	VM	VM	VM	VM
End-to-end service mgmt.	Yes	Yes	Yes	Yes	Yes
Distributed infrastructure	Yes	Yes	Yes	Yes	Yes
Traffic steering	Yes	Yes	Yes	No	Yes
Runs on the network edge	Yes	No	No	No	No
SFC support	Yes	Yes	Yes	No	Yes
Roaming VNFs	Yes	No	No	No	No

In [2], there were highlighted some basic features of containerized VNFs that were measured on an Intel i7 server with 16 GB of memory: Delay: maintaining the low delay introduced by VNF is important to implement transparent services and is therefore a key benchmark for VNF technologies. In Figure 2a, the delay introduced by different virtualization platforms by displaying the idle time (round time trip) is expressed. While ClickOS [8] achieves a slightly lower delay than containers, ClickOS is built on top of a modified, specialized hypervisor that optimizes packet forwarding performance. On the other hand, container-based functions use unmodified containers on a standard Linux kernel, allowing deployment on devices that do not support hardware virtualization (for example, all CPE devices and home routers). Other VM-based technologies, such as KVM or Xen VM, result in a much longer delay, which is mainly attributed to copying packages from the hypervisor to the VM.

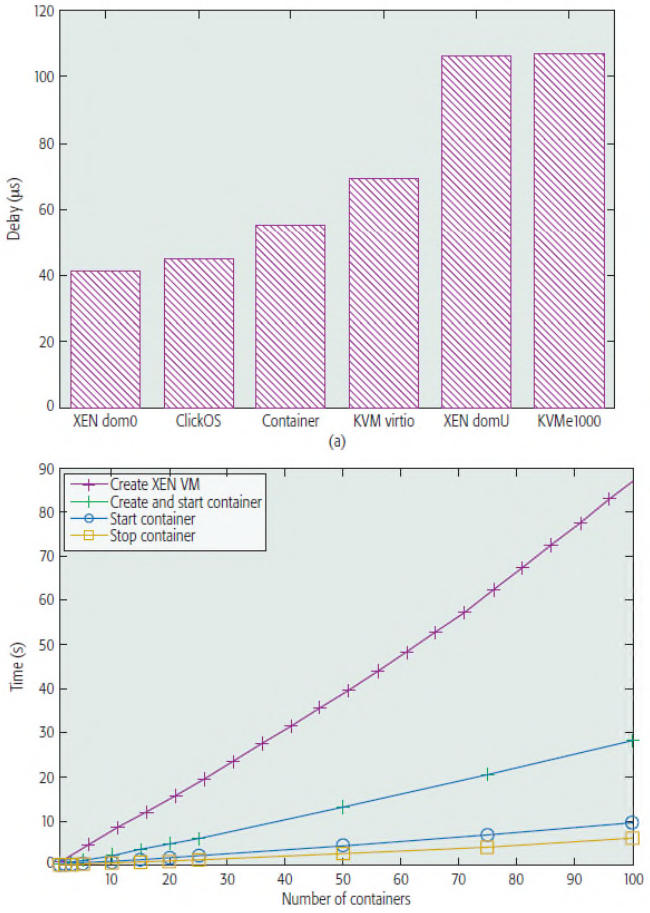


Figure 7. Performances of virtual functions as containers: a) ping delay; b) creation, start and stop times; c) idle memory consumption [2]

V. CONCLUSION

Containers give a false sense of security. There are many pitfalls when it comes to securing applications. It is wrong to assume that one way to secure them is to place them in containers. Containers do not provide anything in themselves. If one keeps his web application containerized, it could be locked into namespaces, but there are several ways to get rid of it depending on his configuration.

Considering that there are Docker images that require the exposure of more than 20 ports for different applications inside a container, Docker's philosophy is that a container

 ISBN: 978-1-61208-837-2

should do a single job and user should compose them instead of making them heavier. If one ends up packing all the tools in one container, all the benefits will be lost, user may have different versions of Java or Python inside, and he might end up with a 20GB image that can not be managed.

The paper managed to provide an overview of the current options for implementing "fog computing": whether it is devices already in production at the end user, or we are talking about native equipment, dedicated to perform functions specific to information processing on the periphery network. Observing these things, a variant that can be adopted is the use of dedicated servers at the periphery of the networks on which to build special functions using Docker technology. This has the advantage of a fast implementation of functions, rapid scaling, as well as the advantage of having a platform shared by many entities given the isolation discussed in Section 4. The problem that remains open is where to implement this dedicated server: it is necessary aggregate and respond to a large number of requests to justify the investment and available computing resources. Physical distance from end users (mobile devices, sensors, etc.) must also be considered in order not to lose the main advantage offered by the concept of "fog computing": latency and low delay.

In this paper, we provided an overview of Docker technology and how this technology can contribute to a better exploitation of virtual network functions. This is because Docker provides very good isolation between instances and at the same time does not require the presence of dedicated software (hypervisor), offering greater flexibility than classic virtual machines.

There are a significant number of benefits to using VNFs on containers rather than on the hypervisor. However, if we look at the technological innovation there is no outstanding progress, and this is due to the lack of a model of common guidelines. Now, 5G networks are starting to be implemented and tested in some cities by service providers with the help of top providers. The development will lead to targeting more innovative features that 5G brings, such as network tracing, Mobile Edge Computing (MEC) and cRAN (Cloud Radio Access Networks). These new 5G features will certainly require the dynamism and benefits offered by containers for the highly automated deployment of services to each edge of the 5G network. We can expect all service providers and network solution providers to be aware of the benefits of the container to be used to achieve high efficiency.

Container technologies such as Docker are becoming the leading standards for building containerized applications. They help organizations free from a complexity that limits the agility of development. Containers, container infrastructure and container implementation technologies have proven to be very powerful abstractions that can be applied to several different use cases. Using something like Kubernetes, an organization can deliver a cloud that uses containers exclusively for application delivery.

The growing interest of users and the widespread adoption of Docker and container technology have forced old retailers to deliver at least their first container products, but it should be noted in the long run how these technologies can integrate seamlessly and meet the technical requirements of old systems.

REFERENCES

[1] S. João, D. Miguel and C. Jorge, "Cloud4NFV: A Platform for Virtual Network Functions," in *in 3rd Intl. Conf. on Cloud Networking (CloudNet). IEEE, 2014*, 2014.

[2] R. Cziva and D. P. Pezaros, "Container Network Functions: Bringing NFV to the Network Edge," in *Communications Magazine. IEEE, June 2017*, 2017.

[3] C. András et al., "Unifying Cloud and Carrier Network," in *Utility and Cloud Computing (UCC), 2013*.

[4] IBM Cloud Education, [Online]. Available: https://www.ibm.com/cloud/learn/containerization. [Accessed 7 March 2021].

[5] Docker Docs, "Docker," [Online]. Available: https://docs.docker.com/get-started/overview/. [Accessed 7 Feb 2021].

[6] F. Rosner, "CodeCentric Blog," [Online]. Available: https://blog.codecentric.de/en/2019/06/docker-demystified/. [Accessed 7 Feb 2021].

[7] X. George et al., "T-NOVA: Network Functions as-a-Service," *IEEE Explore,* 2015.

[8] M. Joao and A. Mohamed, "ClickOS and the Art of Network," in *11th USENIX Symposium on Networked Systems*, Seattle, WA, USA, 2014.

 ISBN: 978-1-61208-837-2