

Determination of the Ideal Protocol Stack for the Transmission of Health Data over 6LoWPAN IoT Networks

S. BİLGİLİ and A. K. DEMİR

Abstract — It is expected that almost every day electronic devices will be connected to the existing internet infrastructure in the context of Internet of Things (IoT). These devices will enable to sense and actuate the physical world. It is foreseen that miniaturized e-health devices will enable monitoring vital health of patients. There exist some studies on networking these e-health devices within the Internet. In this realm, several network protocols are being standardized. 6LoWPAN of IETF is one of these efforts where some set of protocols can be stacked over IEEE 802.15.4 radio. However, it is not clear that which ideal protocol stack for transmission of health data can be adopted well. The novelty of this work is that we studied determination of ideal protocol stack for transmitting health data over 6LoWPAN IoT networks. So then, we carried extensive simulations over Cooja simulator. The compelling results are presented in this work. The results show that 6LoWPAN IoT health networks can be used to serve vital health data of patients.

Index Terms—Internet of Things, 6LoWPAN, Medium Access Control, Radio Duty Cycling, CoAP.

I. INTRODUCTION

TANY of the current everyday electronic devices in use are able to exchange data autonomously. These devices can network among themselves as well as connect to an existing Internet network. The concept of the Internet of Things is the general name given to this structure [1], [2]. Devices within this scope are mostly low-cost and limited devices. IoT devices generally obtain data from their surroundings with the help of sensors on them. These devices send the data they receive to a center for processing or perform some other operations. Connecting each of these devices directly to the Internet will incur additional costs. To avoid this, generally, IoT devices primarily form a network within themselves. A

gateway node within the scope of this network acts as a bridge between the Internet and the IoT network.

The IoT concept is currently used in smart home/office systems, factory production lines, smart agricultural systems, smart city/traffic systems. In the future, it is envisaged that IoT systems will become more widespread and expand into more areas. The lightweight and portable IoT devices has being introduced IoT concept into the healthcare sector. Especially for health monitoring, their portability and low-power features have made IoT devices the preferred choice.

Although the IoT concept is currently in use in many areas, it is still a developing technology. Therefore, there are no emerged de facto standards yet. Although wireless technologies such as Wi-Fi, Bluetooth and GSM can also be used for the IoT environment, the power saving offered by 802.15.4 wireless technology is more suitable and common for IoT systems. For energy-saving IoT devices, hardware is also constrained to keep the energy consumption low. Therefore, instead of protocols with high system requirements, lightweight protocols are being proposed and standardized. One of these efforts is 6LoWPAN working group of IETF. 6LoWPAN seems like providing promising IoT network standards and protocols [3].

Typical 6LoWPAN standard network layers and protocols of IoT devices is given in **Hata! Başvuru kaynağı bulunamadı..** In this layered structure, the protocols in the transport, network and application layers are almost standardized and widely used. However, the protocols used in the data link layer needs to be selected according to application quality of service (QoS) requirements. Therefore, selection of ideal protocol stack for applications requires careful research.

In this work, careful determination of the ideal protocol stack for e-Health application is investigated. As is known, e-Health applications are sensitive to delays. Therefore, timely transmission and hand off e-Health data to a distant center are core QoS requirements of e-Health applications. Besides, an e-Health application may need different health sensors such as ECG, EMG, Blood Pressure, Body Temperature and Body Position etc. Each health sensor requires different maximum delay thresholds. This can vary from seconds to hours. Moreover, maximum delay thresholds may also vary for different patient categories such as critical, non-critical and follow-up patients. Thus, to achieve this, we investigated the performance of different protocol stack of MAC and RDC

SEDAT BİLGİLİ, is with Department of Computer Engineering Adana Alparslan Turkes Science and Technology University, Adana, Turkey, (e-mail: sbilgili@atu.edu.tr).

 <https://orcid.org/0000-0001-6708-7209>

ALPER KAMİL DEMİR, is with Department of Computer Engineering Adana Alparslan Turkes Science and Technology University, Adana, Turkey, (e-mail: akdemir@atu.edu.tr).

 <https://orcid.org/0000-0002-9256-0368>

Manuscript received November 07, 2019; accepted March 16, 2020.
DOI: [10.17694/bajece.644104](https://doi.org/10.17694/bajece.644104)

layer of an e-Health application for different patient categories so that patient's vital health data can be monitored smoothly.

Transmission of e-Health data over IoT networks is fairly a new research subject. Thus, there does not exist satisfying results in the literature and applications. The novelty of this work is that e-Health data is transmitted with standard CoAP application layer protocol and the effect of performance belonging to MAC and RDC layer protocols, such as CSMA and contikiMAC, are explored with simulation of real network and hardware. Furthermore, the network topology and the number of patients (clients) equipped with e-Health sensors are varied with extensive simulations.

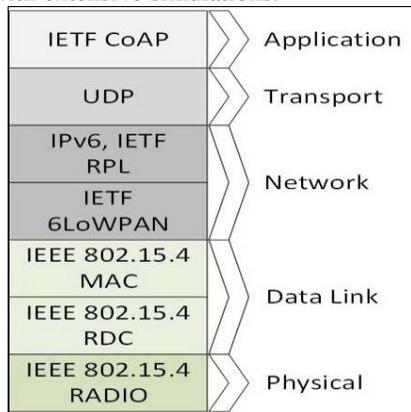


Fig.1. Network Layers in IoT

This paper is organized as follows: In section II we surveyed related works that are associated to subject of this paper. Our methods are provided in section III. Based on these methods, we investigated results in section IV. In section V, we provided conclusion and future work.

II. RELATED WORK

The transmission and processing of vital health data in IoT environments are emerging research subject that is being explored scarcely yet. The IoT for healthcare is broadly surveyed in [4], [5]. However, there does not exist a comprehensive survey of transmitting health data in 6LoWPAN IoT networks. Moreover, there does not exist concrete study on transmitting health data in 6LoWPAN IoT networks. We briefly talk about networking health data over 6LoWPAN IoT networks in this section.

Sphere framework [6] brings 6LoWPAN IoT standards for healthcare to the home. The initial outcomes exhibit good 6LoWPAN network performance to carry out healthcare data (99.97 percent average PDR).

IoT net platform [7] anticipates technological solutions for healthcare protection and services through trendy 6LoWPAN IoT networks. In [8], again, analysis of 6LoWPAN IoT network is provided for maternal healthcare. It is concluded that both CoAP and 6LoWPAN could be applied for healthcare monitoring. The research in [9] demonstrates that 6LoWPAN IoT network is able to be used for healthcare services with CoAP.

The initial research views that 6LoWPAN IoT networks are promising solution to be used in healthcare applications. However, as it is seen that the usage of 6LoWPAN IoT

networks in healthcare domain is an unexplored area. We extend this gap furtherly in this work.

III. METHODOLOGY

Within the scope of this section, we present the methodology of our work to transmit vital health data over a 6LoWPAN IoT network. The details are as follows:

A. Obtaining Health Data

Although performance evaluations of this work is executed on a simulation environment, real world health data is required to get realistic results. To achieve this, MySignals health sensor kit is used with various additional hardware, Arduino Uno microcontroller and Raspberry Pi microcomputer as seen in Fig. 1. MySignals health sensor kit is programmed with a simple firmware to get all sensor data. Various sensor data is collected from various persons to ensure collected data is realistic.

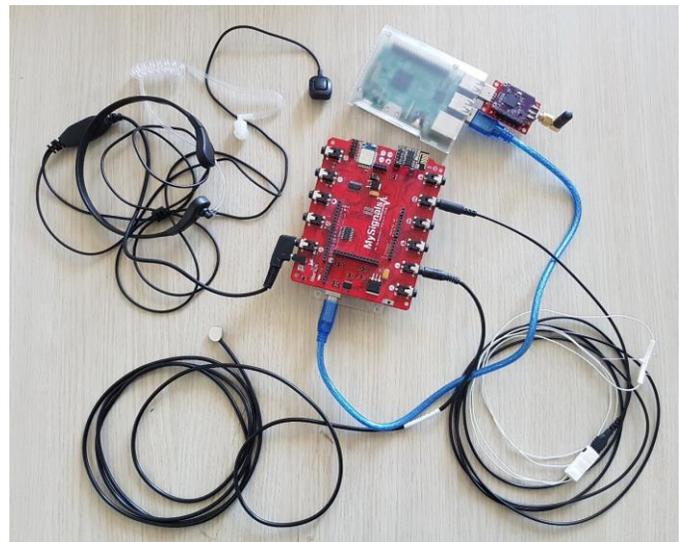


Fig. 1. eHealth Sensor Kit

B. Health Data Traffic Characteristics

Right after obtaining real-world health data, each sensor data is composed into a packet. Each health data is encapsulated into 64-byte packet. Each packet contains data from all available health sensors. Sensor data types and their length is given in Table I. In this work, although we used all available health sensors, there's 20 bytes free space in packet which can be used for patient information or extra sensors. These eHealth data packets are updated in memory dynamically every 300ms. The clients send CoAP CON messages to obtain eHealth data. Respectively, the server nodes send piggybacked CoAP ACK messages that contain eHealth data whenever they receive a CoAP CON message.

Table I Contents of eHealth Data Packet

ID	Sensor	Bytes
----	--------	-------

1	Body Position	6
2	Body Temperature	2
3	Snore Sensor	3
4	Galvanic Skin Response	8
5	Airflow Sensor	2
6	EMG Sensor	2
7	ECG Sensor	2
8	SPo2	4
9	Blood Pressure Sensor	6
10	Body Scale	2
11	Glucometer	6
12	Patient ID	1
	Total	44
	Free Space	20

C. Latency QoS Requirement of Health Data

We envisioned that each eHealth sensor data needs to be transmitted within a maximum latency deadline. Thus, we talked a couple of medical doctors to detect latency deadline of eHealth data. According to interviewed medical doctors, patients should be divided into three groups, critical, non-critical and follow-up patients, as they may have need different latency deadlines. As a result, maximum latency deadline values are given in Table II. These values represent the maximum latency tolerance of eHealth data generated by health sensors. For example, a critical patient's consecutive ECG sensor data needs to be transmitted within 1 minute. On the other hand, ECG sensor data demand maximum 60 minutes latency for non-critical and follow-up patients. Moreover, body position data requires maximum 30 minutes latency for critical and non-critical patients.

Table II eHealth Data Maximum Latency Deadlines

Sensor	Patient Category		
	Critical	Non-Critical	Follow-up
Body Position	30	30	15
Body Temperature	15	30	60
Snore Sensor	30	60	60
Galvanic Skin Response	60	60	60
Airflow Sensor	30	30	60
EMG Sensor	1	60	60
ECG Sensor	1	60	60
SPo2	1	60	60
Blood Pressure Sensor	30	60	60
Body Scale	60	60	60
Glucometer	60	60	60
Deadline 1: 1 minute			
Deadline 2: 15 minutes			
Deadline 3: 30 minutes			
Deadline 4: 60 minutes			

D. Simulation Environment

We used Cooja [10] network simulator that simulates multiple types of nodes and network software running on nodes. Cooja simulator mimics ContikiOS [11] operating system designed for IoT devices. Also, Cooja network simulator offers multiple measurement tools. WisMote is used as a hardware server and gateway node in simulations within IoT network. These server nodes generate sampled eHealth data traffic. Californium [12] is used as CoAP client running on real PC hardware and requiring eHealth data piggybacked in CoAP ACK messages. In other words, CoAP servers, running on simulated IoT network, are programmed with Erbium [13] implementation of CoAP, and CoAP clients, running on real PC, are programmed with Californium implementation of CoAP. The simulated IoT network topology is given in Fig. 2. The distance between each node is about 40 meters.

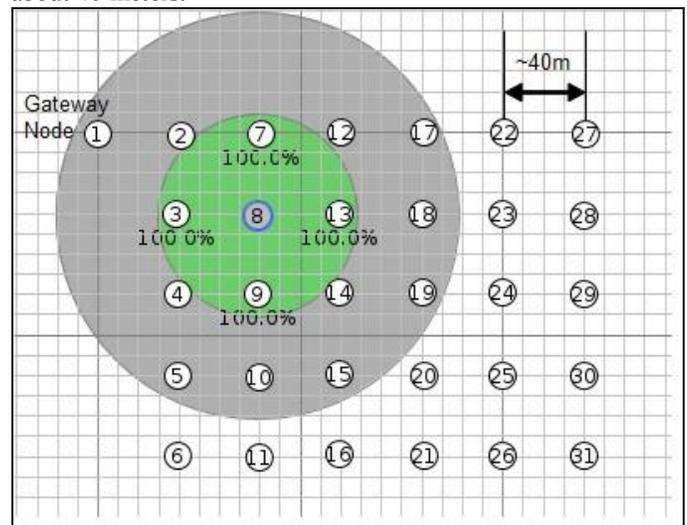


Fig. 2. IoT Network Topology in Simulations

CSMA and nullMAC protocols are varied at MAC layer. And, contikiMAC and nullRDC protocols are varied at RDC layer. Moreover, PDR values are ranged as 90, 95 and 100. This enabled us to simulate 12 different scenarios (2x2x3). The number of clients is varied from 2 to 30 stepped by 2 (2,4,6,...,30). The number of servers is always the same as the number of clients. The positions of servers are detected according to their relative position to the gateway node. Always, the closest nodes are selected as a server. Each client sends totally 100 CoAP CON requests. Each server replies with CoAP ACK message as soon as it gets CoAP CON request. The total elapsed time is to transmit 100 CoAP CON messages. According to CoAP standard, the default maximum re-transmission of lost CoAP CON packets is 4 times. One thing to keep in mind is that CoAP handles a default congestion control mechanism.

E. Performance Metrics

To inspect how well health data is transmitted in an IoT network, we need some measurable performance metrics. In this sense, we identified 3 different performance metrics, latency, energy efficiency and reliability. We give the definition of each performance metric below.

1) Latency

Latency metric defines the time elapsed between two consecutive CoAP ACK messages. As the subject of this work is health data, it means that the data must be transmitted within deadline time limits. These time limits are shown in Table II.

2) Energy Efficiency

Energy efficiency metric is used to represent the amount of energy consumed by a server node. This metric is calculated as the average of consumed energy of all server nodes. Indirectly, this metric shows the overall network life time.

3) Reliability

Reliability metric demonstrates the percentage of successfully received CoAP ACK messages. Higher reliability means that eHealth data is smoothly displayed at health center. The low reliability may result with low perceived health data.

IV. PERFORMANCE EVALUATION

In this section, we investigate the performance of 12 scenarios, given at Section III.D based on 3 different performance metrics.

A. Latency Evaluation

As stated earlier, health data should be transmitted within a certain period of time. Time limits for different health sensors and patient groups are shown in Table II. The graphs in this section show the performance indicators as well as the latency deadline indicators. Thus, it is possible to determine how many clients can be supported by the specified latency deadline in a given protocol stack. Please note that if there's no latency deadline indicator for a performance indicator, it means that all results in the graph comply with absent latency deadline.

Various simulations were performed for different protocol stacks. **Fig. 3** shows the latency graph with protocol stack of nullMAC and nullRDC in MAC and RDC layers respectively. As can be seen in the graph, all results are lower than deadline of 30 and 60 minutes (Hence, these deadline indicators are not shown in the graphs). All number of clients, other than 26 and 30, comply with deadline limit of 15 minutes. Therefore, the network can support up to 24 clients. For example, body temperature sensor data can be used safely for all patient groups up to 24 patients. However, for more critical data with deadline limit of 1 minute, only 8 clients can be serviced when PDR equals to 100.

Fig. 4 shows latency graph of CSMA and nullRDC protocols. As it is seen, deadline limits of 15, 30 and 60 minutes are missing in the graph because all latency values are lower than 15, 30 and 60 minutes. Therefore, only 1 minute latency indicator is given in the graph. For all PDR values, up to 16 clients can be monitored without any trouble. However, for example, when the client number is above 20 the network is not able to support health data with 1 minute latency deadline.

In **Fig. 5**, nullMAC and contikiMAC combinations are used for latency deadlines. Accordingly, for 30 minute latency, only up to 18 clients can be handled. Besides, for 15 minute latency, individually up to 8 clients can be supported. Nevertheless, for 1 minute latency, only 2 clients with PDR values 100, can be serviced.

CSMA and contikiMAC protocol combination latency graph which is given in **Fig. 6** shows that 24 clients can be monitored for latency deadline of 30 minutes. Based on the figure, for latency deadline of 15 minutes, there can be only 16 clients. More drastically, latency deadline of 1 minute can only support 4 clients.

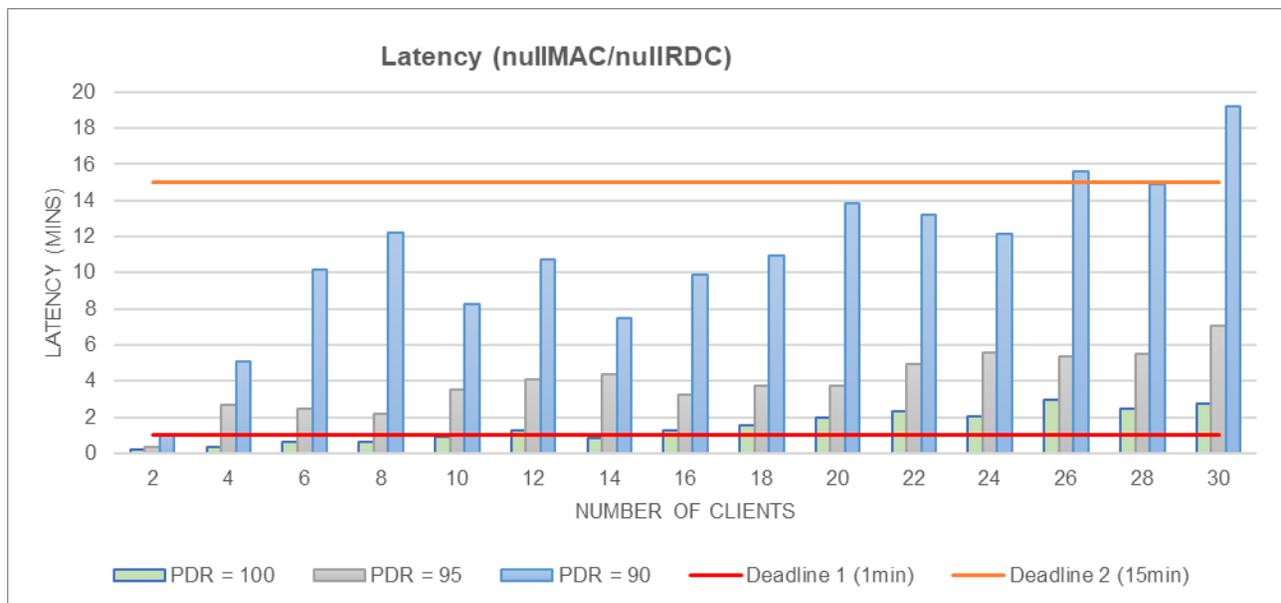


Fig. 3. Latency Graph for nullMAC/nullRDC Protocols

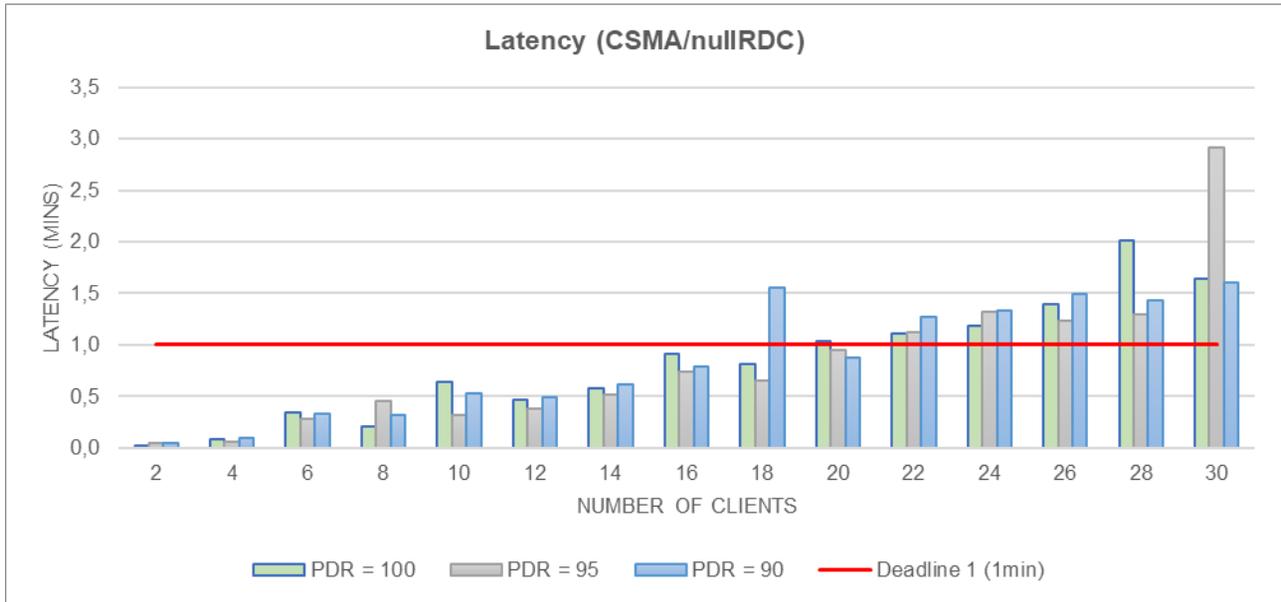


Fig. 4. Latency Graph for CSMA/nullRDC Protocols

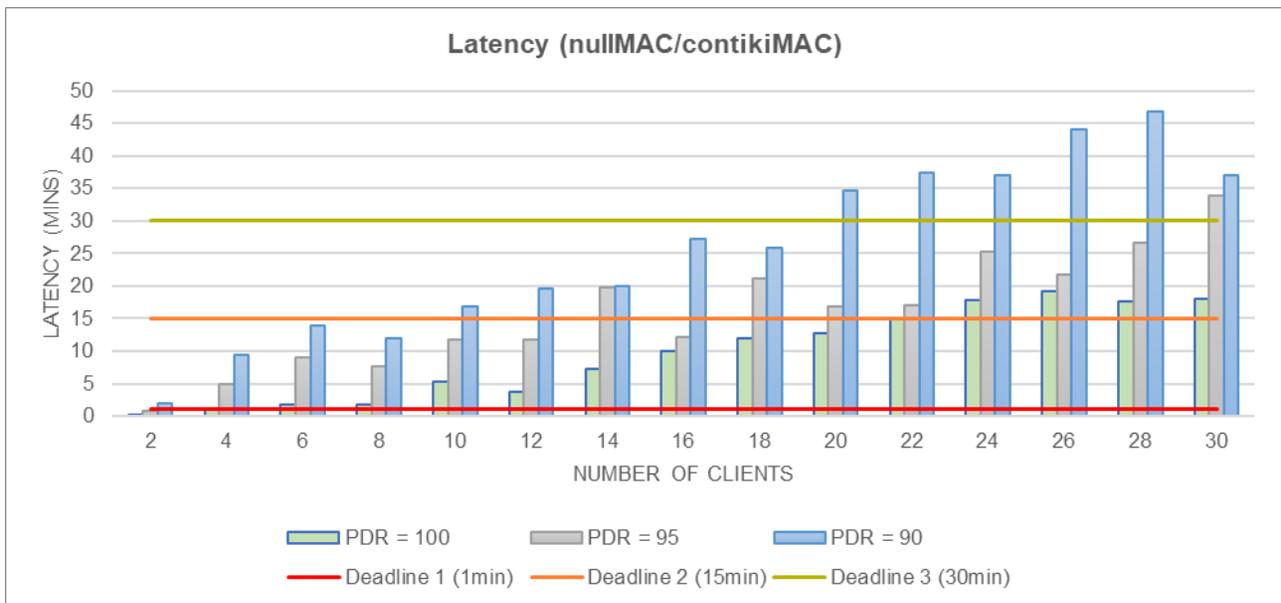


Fig. 5. Latency Graph for nullMAC/contikiMAC Protocols

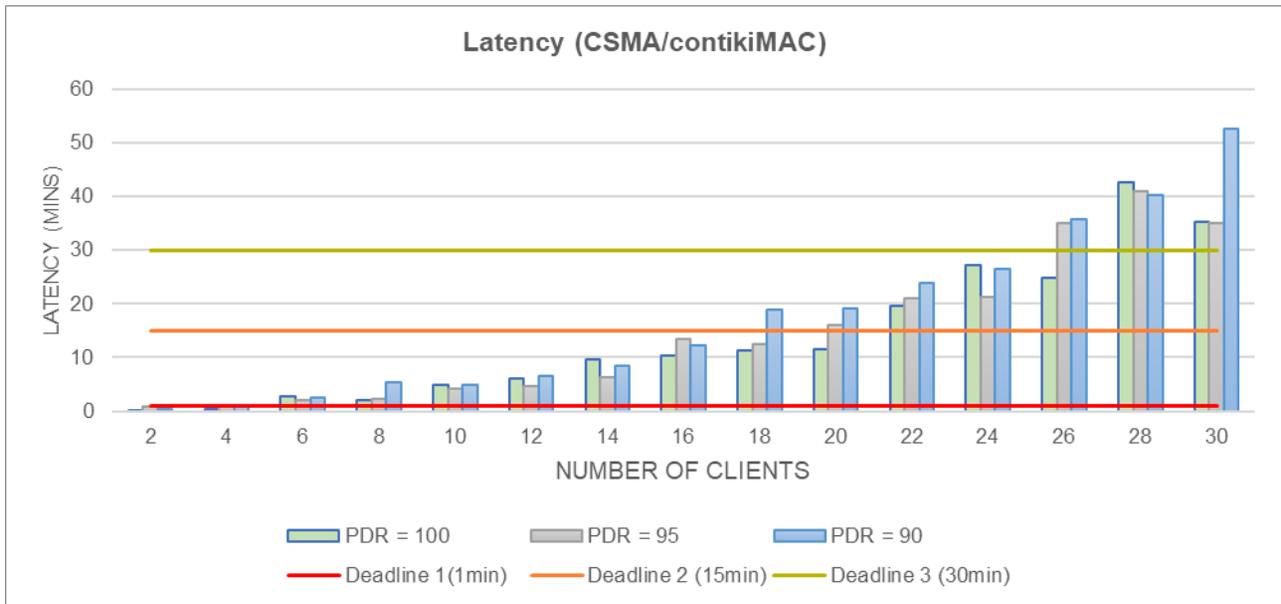


Fig. 6. Latency Graph for CSMA/contikiMAC Protocols

B. Energy Efficiency Evaluation

In this section, we investigate the energy efficiency of MAC and RDC layer protocol combinations.

Fig. 7 shows the energy consumption comparison of 4 protocol combinations when the PDR value is 100. Apparently, when nullRDC is used, the energy consumption significantly increases. Because while using nullRDC, 802.15.4 radio does not sleep when it is idle. Thus, it uses more energy. In contrast, contikiMAC sleeps the radio while it's idle. The effect of this mechanism can also be observed in the graph. Using CSMA or nullMAC protocol with nullRDC has almost the same energy consumption. However, while using contikiMAC protocol, selecting CSMA protocol causes

more energy consumption against selecting nullMAC protocol.

Energy consumption values while PDR value is 95 is given in Fig. 8. Again, selection of contikiMAC in RDC layer significantly decreases energy usage. The results show similar curve with previous graph. However, difference between nullMAC/nullRDC and CSMA/nullRDC combinations is much more distinctive when PDR is 95.

In Fig. 9, energy consumption values for PDR value 90 is presented. Based on the graph, again, it is clear that contikiMAC protocol provides more energy savings. As can be seen, for protocol combinations with nullRDC, energy consumption values get higher as the PDR value decreases.

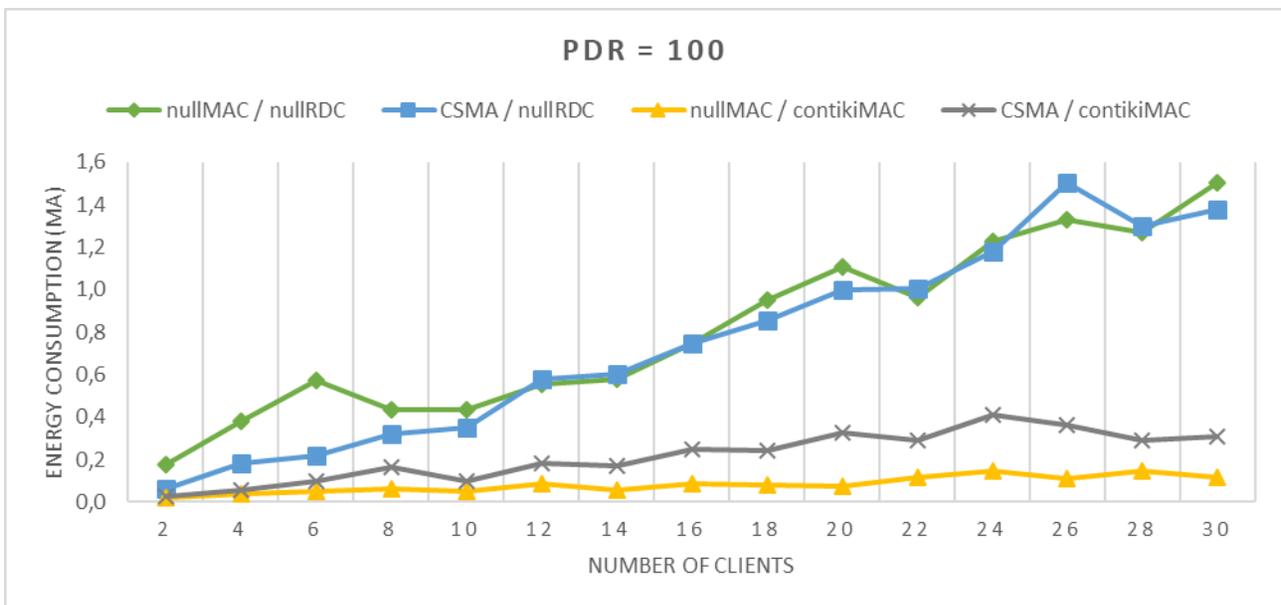


Fig. 7. Average Energy Consumption for PDR value = 100

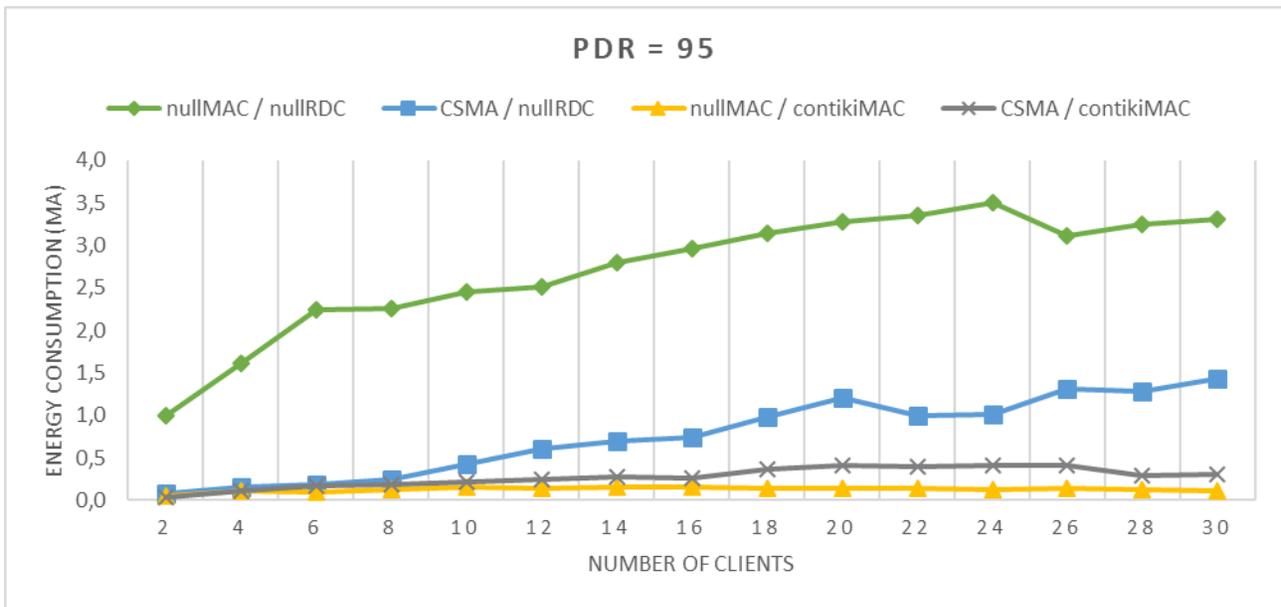


Fig. 8. Average Energy Consumption for PDR value = 95

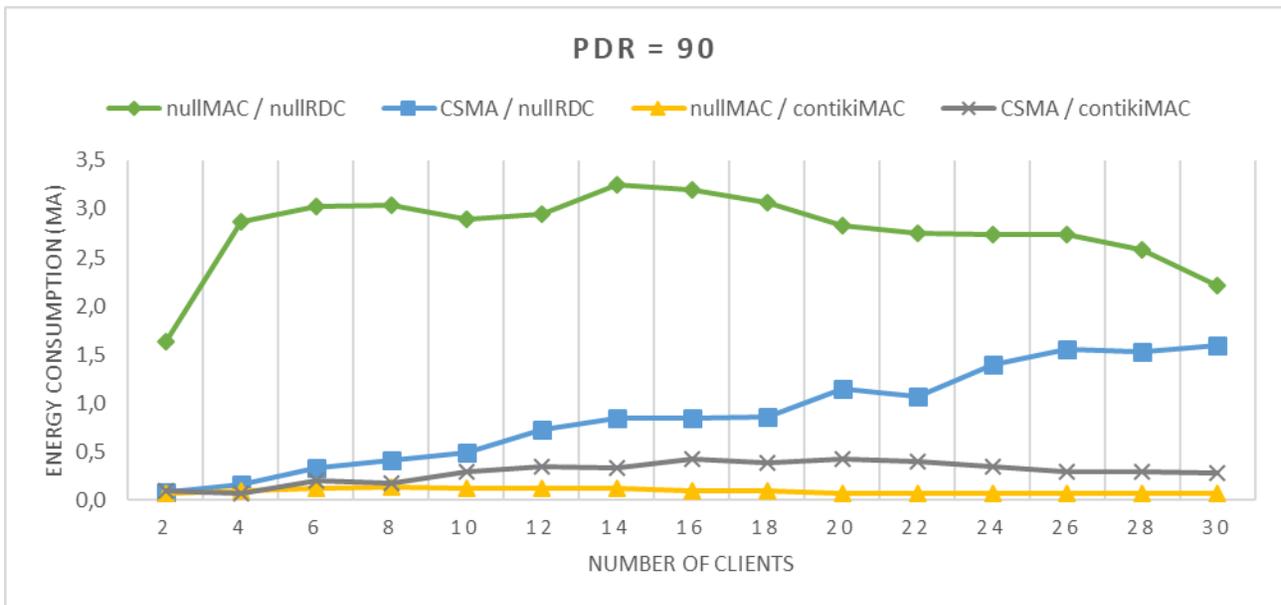


Fig. 9. Average Energy Consumption for PDR value = 90

C. Reliability Evaluation

In this section, reliability metric values are presented. These values show the rate of successfully transmitted health data packets. The four protocol combinations (nullMAC/nullRDC, CSMA/nullRDC, nullMAC/contikiMAC and CSMA/contikiMAC) are compared with different PDR values.

Reliability values when the PDR value is 100 is given in

Fig. 10. That graph shows that CSMA and nullRDC protocol combination gives better results. Besides, nullMAC and nullRDC protocol combination has results that are close to CSMA and nullRDC protocol combination. However, nullMAC and contikiMAC protocol combination cannot sustain reliability as the client number increases. CSMA and

contikiMAC protocol combination gives the worst reliability especially for high number of clients.

PDR value of 95 is given in

Fig. 11. As the client number increases, the gap between nullMAC/nullRDC and CSMA/nullRDC protocol combinations increases. CSMA/nullRDC gives the best performance compared to other three combinations. The graph shows that using CSMA protocol is helpful as CSMA maintains reliability high.

When PDR value equals 90, the same reliability performance is observed. Results are presented in Fig. 12. Once more, absence of CSMA protocol in protocol stack causes lower reliability results. Using CSMA is superior than using nullMAC cause CSMA protocol successfully

retransmits lost frames. Using CSMA protocol with contikiMAC protocol gives undesired results when the number of clients increases. This is due to the fact that contikiMAC

protocol sleeps radio to save energy, so CSMA protocol must wait for these sleep intervals.

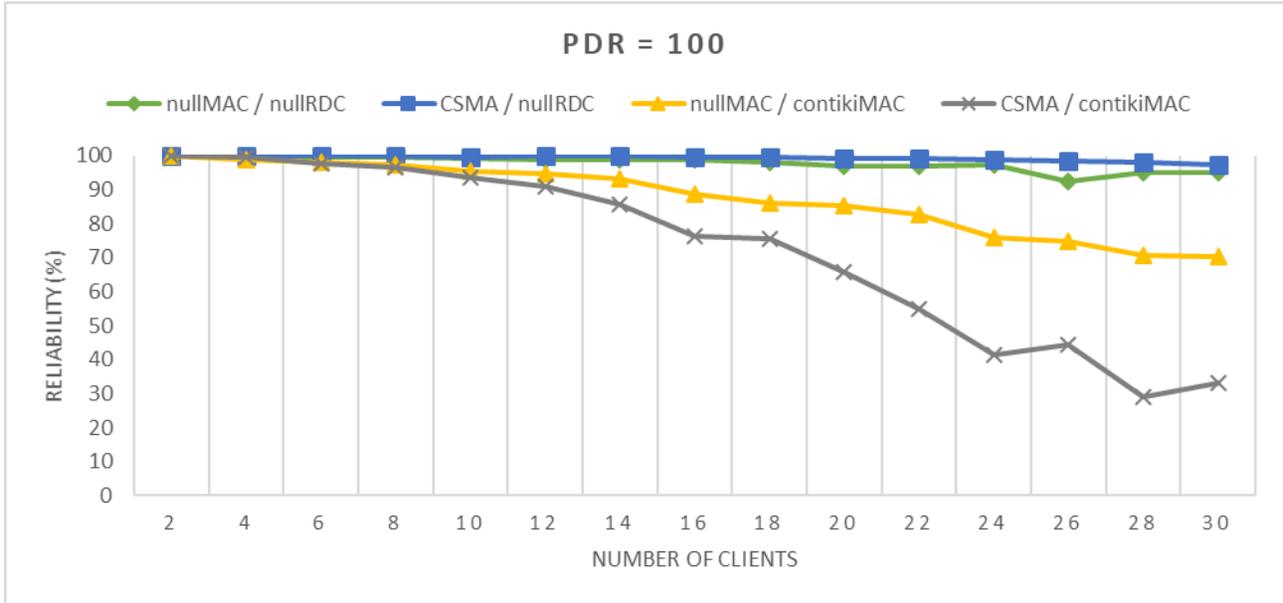


Fig. 10. Success Ratio/PDR value = 100

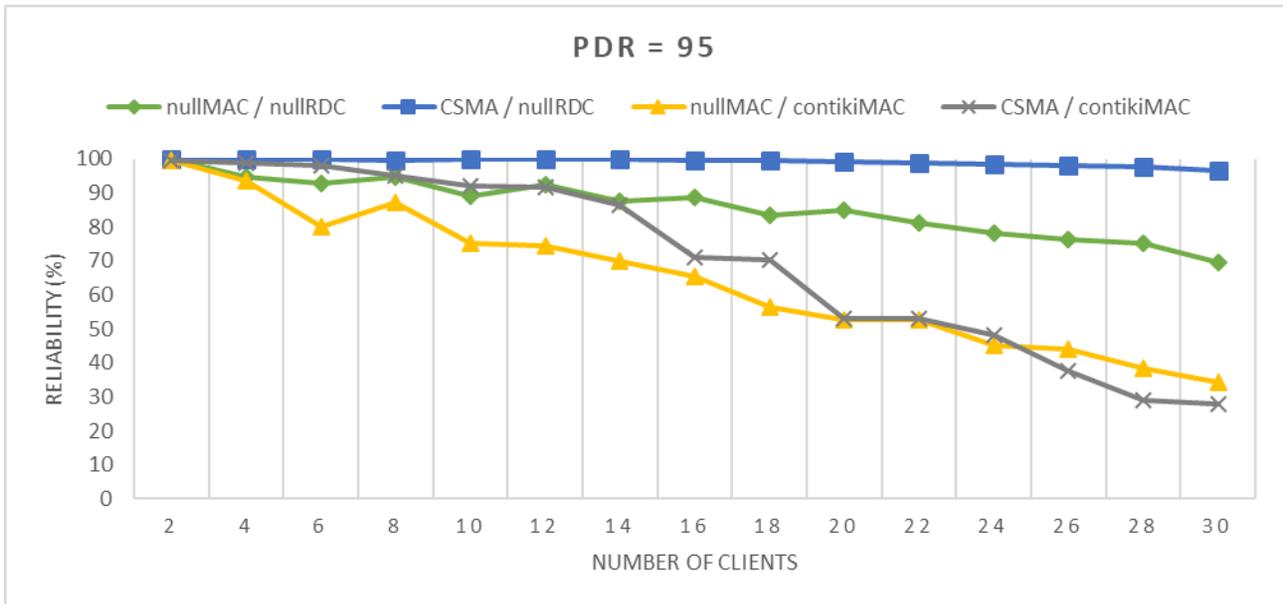


Fig. 11. Success Ratio/PDR value = 95

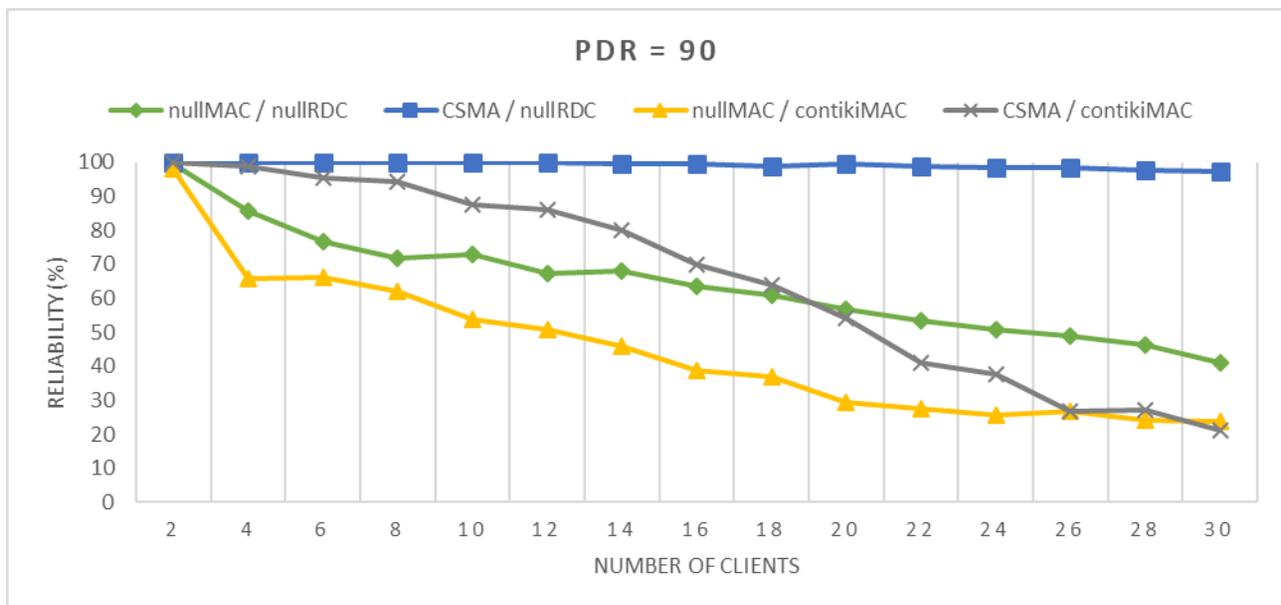


Fig. 12. Success Ratio/PDR value = 90

V. CONCLUSION AND FUTURE WORK

In this work, we investigate determination of ideal protocol stack for transmission of health data over 6LoWPAN IoT networks. Our extensive work shows that 6LoWPAN IoT networks are able to transmit vital health data of patients up to a certain point. Latency, reliability and energy efficiency graphs are analysed to determine the maximum patient number that can be supported in a 6LoWPAN IoT network.

Ideal protocol combination may differ based on patient category and health sensor. Although nullRDC protocol in RDC layer seems to show better performance, it results with inefficient energy consumption. Therefore, choosing ideal protocol combination highly depends on latency, reliability and energy efficiency performance results. For instance, even if CSMA/nullRDC combination can support up to 16 patients for critical health data in 6LoWPAN IoT network, energy consumption significantly gets higher.

In future, the more extensive simulations can be carried out by varying IoT network topology and PDR values. Routing protocol, RPL (especially RPL Objective Functions), is not investigated in this work to expose its effect on the performance. Moreover, only CoAP is used as an application layer protocol as it is the only candidate for now in IETF. Other being standardized protocols, such as MQTT, can also be considered. The least but not the last, CoAP promotes other congestion control mechanisms, such as CoCoA. Using different congestion control mechanisms to determine ideal protocol stack can also be inspected.

ACKNOWLEDGMENT

This work was supported by SIREN project funded by the Scientific and Technological Research Council of Turkey (TUBITAK) under Grant No 116E025 and by Tiktak project funded by Scientific Research Projects (BAP) Coordination of Adana Alparslan Turkes Science and Technology University under Grant No 16103002.

REFERENCES

- [1] L. Atzori, A. Iera, and G. Morabito, "The internet of things: A survey," *Comput. networks*, vol. 54, no. 15, pp. 2787–2805, 2010.
- [2] V. Gazis, "A Survey of Standards for Machine-to-Machine and the Internet of Things," *IEEE Commun. Surv. Tutorials*, vol. 19, no. 1, pp. 482–511, 2017.
- [3] Z. Shelby and C. Bormann, "Introduction, in 6LoWPAN: The Wireless Embedded Internet," in *6LoWPAN*, John Wiley & Sons, Ltd, 2009, pp. 1–25.
- [4] D. A. Gandhi and M. Ghosal, "Intelligent Healthcare Using IoT: A Extensive Survey," *Proc. Int. Conf. Inven. Commun. Comput. Technol. ICICCT 2018*, no. Icicct, pp. 800–802, 2018.
- [5] H. Ahmadi, G. Arji, L. Shahmoradi, R. Safdari, M. Nilashi, and M. Alizadeh, *The application of internet of things in healthcare: a systematic literature review and classification*, vol. 18, no. 4. Springer Berlin Heidelberg, 2018.
- [6] A. Elsts *et al.*, "Enabling Healthcare in Smart Homes: The SPHERE IoT Network Infrastructure," *IEEE Commun. Mag.*, vol. 56, no. 12, pp. 164–170, 2018.
- [7] E. L. Lydia, K. Shankar, M. Ilayaraja, and K. S. Kumar, "Technological Solutions for Health Care Protection and Services Through Internet Of Things(IoT)," *Int. J. Pure Appl. Math.*, vol. 118, no. 7 Special Issue, pp. 277–282, 2018.
- [8] K. Kabilan, N. Bhalaji, and S. Chithra, *Analysis of 6LoWPAN and CoAP protocols for maternal health care*, vol. 521. Springer Singapore, 2019.
- [9] J. Hwa Jung, D. Kyu Choi, J. In Kim, and S. Joo Koh, "Mobility management for healthcare services in coap-based iot networks," *Int. Conf. Inf. Netw.*, vol. 2019-Janua, pp. 7–12, 2019.
- [10] A. Sehgal, "Using the contiki cooja simulator," *Comput. Sci. Jacobs Univ. Bremen Campus Ring*, vol. 1, p. 28759, 2013.
- [11] A. Dunkels, O. Schmidt, N. Finne, J. Eriksson, F. Österlind, and N. T. M. Durvy, "The contiki os: The operating system for the internet of things," *Online*, <http://www.contikios.org>, vol. 605, 2011.
- [12] M. Kovatsch, M. Lanter, and Z. Shelby, "Californium: Scalable cloud services for the internet of things with coap," in *2014 International Conference on the Internet of Things (IOT)*, 2014, pp. 1–6.
- [13] M. Kovatsch, S. Duquennoy, and A. Dunkels, "A low-power CoAP for Contiki," *Proc. - 8th IEEE Int. Conf. Mob. Ad-hoc Sens. Syst. MASS 2011*, pp. 855–860, 2011.

BIOGRAPHIES



SEDAT BILGILI is a Research Assist. at Computer Engineering Department of Adana Alparslan Turkes Science and Technology University. He is also a PhD. student at department of Electrical and Electronics Engineering, Adana Alparslan Turkes Science and Technology University. He received his BS degree from Cukurova University, Adana, Turkey in 2015. He worked at BSD Inc. as a Network Administrator between 2015–2016. He receives MSc. Degree from Adana Alparslan Turkes Science and Technology University, Adana, Turkey in 2019. His master thesis was on Healthcare in Internet of Things. He is interested in Internet of Things, Information Centric Networking, Embedded Systems and Computer Networks. He is also interested in Arduino, Raspberry Pi, general sensors and electronics as a hobbyist.



ALPER K. DEMIR is an Assist. Prof. at Computer Engineering Department of Adana Alparslan Turkes Science and Technology University. He received his BS degree from Hacettepe University, Ankara, Turkey and MS degree from University of Southern California (USC), Los Angeles, USA, and PhD degree from Kocaeli University Kocaeli, Turkey in 1993, 1998 and 2013 respectively. Between 2009–2013, he worked at Huawei Telecommunications Inc. as a Senior Software and Research Engineer. Between 2001–2009 he worked at Kocaeli University, Computer Engineering Department as a Senior Instructor. He is interested in Computer Networks, Distributed Systems and Operating Systems in general. Currently, his research is focused on Internet of Things.