Contents lists available at ScienceDirect

Measurement: Sensors

journal homepage: www.sciencedirect.com/journal/measurement-sensors

End-to-end security in embedded system for modern mobile communication technologies

D. Venu [a,*], Babu J [b], R. Saravanakumar [c], Ricardo Fernando Cosio Borda [d], Yousef Methkal Abd Algani [e,f], B. Kiran Bala [g]

[a] *Department of ECE, Kakatiya Institute of Technology and Science, Warangal, India*
[b] *Department Electronics and Communication Engineering, Dadi Institute of Engineering & Technology, Anakapalle, India*
[c] *Department of Wireless Communication, Institute of ECE, Saveetha School of Engineering, Saveetha Institute of Medical and Technical Sciences, Chennai, India*
[d] *Universidad Autónoma del Perú, Lima, Peru*
[e] *Department of Mathematics, Sakhnin College, Israel*
[f] *Department of Mathematics, The Arab Academic College for Education in Israel-Haifa, Israel*
[g] *Head of the Department, Department of Artificial Intelligence and Data Science, K.Ramakrishnan College of Engineering, Trichy, Tamil Nadu, India*

ARTICLE INFO

Keywords:
IoT
Security
Mobile communication
Privacy
Embedded system

ABSTRACT

Modern mobile electronic devices such as smartphones or cell phones can now be used for distant devices such as technical systems to monitor and control. While surveillance systems do not require high standards navigating about the time of transfer of the displayed data. More real-time data are needed for a remote mobile robot transfer. Therefore, it has investigated and measured not only the possibilities of employing mobile devices. But also, the supported data transmission channels, such as UMTS, GSM, Wireless LAN, and Bluetooth. The remote-control system is used in many applications such as smart homes, cities, smart hospitals, etc., but it must be today updated to ensure fast-changing technology. Extensive coverage, remote control, and reliable operation in real-time in the deployment of wireless security knowledge. The home automation control system delivers significant features together with a user-friendly interface. A secure remote-based end-to-end security system NTMobile, a technique that enables NAT to provide transverse and encrypted communication from end to end. This confirmed that evaluating the performance of the system in the ECHONET lite compatible smartphone ecosystem. This gives flexibility in configuring time-sensitive industrial networks and enables them to be secured. A safe and reliable remote-control system is also conceivable under the privacy of the user.

1. Introduction

The global wireless communication trend has increased to broadband data rather than the simple voice. While the communication network is readily accessible, the real-time data reporting architecture benefits remote monitoring and control. Appropriate media with analog and digital data transmission capabilities should be selected to transmit data wirelessly. Media having crucial restrictions are diverse in UHF, VHF, or HF [1]. Real-time control or surveillance can be hard to design livelihood applications. Wireless modems were a popular choice for distant communication and control. However, the wireless modem lacks in application because of the power and range limit. ECHONET Lite is the most widely known controlling and management as standard protocol such devices in Japan. Home device makers establish an internet support server for the remote control to achieve these services [2].

Modern mobile phones or even the newly popular mini netbooks support several wireless technologies in the field of data communication. Alongside the carrier, Bluetooth and wireless LAN networks like GPRS and EDGE are also supported by practically every modern smartphone, as are UMTS with and without HSDPA [3]. This advancement of recent years has increased the likelihood of unbound remote control, together with the capacity to run. A modern and smart technician can reach the aim everywhere systems. The same equipment might be wireless using Bluetooth or LAN if it is near the device operated using GSM or UMTS mobile devices [4]. The researchers have described the

* Corresponding author.
E-mail addresses: dunde.venu@gmail.com (D. Venu), jettisanjay@gmail.com (B. J), saravanakumarr.sse@saveetha.com (R. Saravanakumar), ricardo.cosio.borda@gmail.com (R.F. Cosio Borda).

https://doi.org/10.1016/j.measen.2022.100393
Received 27 May 2022; Received in revised form 12 July 2022; Accepted 13 July 2022
Available online 19 July 2022

various wireless systems technologies for the data connections and a prototype of a mobile robot remote control service on mobile equipment.

The remote-control support (RCS) internet-installed server, which provided the ECHONET lite control service, cooperates. The services will improve the quality of energy (QoE) and the prevention of crime. For remote control services, manufacturers must operate the RCS server stably [5]. But once the services are completed, even if the controller is in use, a user cannot control the external devices. If log information is hacked out of the RCS server. A supplier may examine user life patterns of a device's business history and may violate user confidentiality, including time information [6].

The Mobile transversal network (NTMobile), capable of solving transversal network address (NAT) issues, then achieving end-to-end IP layer Migration encoding communications. In addition, terminals communicate over the UDP tunnel. Due to the encryption and authentication of the communication material at the IP level [7]. That offers a solution with the use of the NTMobile, which can deploy ECHONET Lite devices safely and securely in the home network. The suggested system corresponds to the ECHONET Lite protocol by expanding the NTMobile specification. The user devices build the UDP tunnel to the RCS using the NTMobile and that send messages in an encryption UDP tunnel to control ECHONET Lite devices [8]. This system may therefore be controlled without any RCS server on the market devices. An android tablet and Linus PC proposed system prototype is installed and a comparative evaluation of the modern mobile communication to remote control services was carried out the mobile internet performance.

The remaining part and the aim of this paper are explained the remote-control system for modern mobile communication; part 2 defines the highlight of the previous effort that can be done by the scholars in this domain with the various experimental tasks; part 3 offering the proposed methodology architecture model and its mechanism, part 4 represents the evaluation and performance of the result and discussion and part 5 represents the work achieved in conclusion.

2. Related work

[9] proposes a smart home remote control platform based on state-of-the-art web technologies that were created and implemented. Intelligent house monitoring and management tasks are integrated into this mobile platform. Smartphones can communicate through the Internet with web servers and connect to intelligent house management systems. The outcome shows that consumers can always and anywhere access electrical equipment, monitor the environment, and security in the home. Smart home systems, the mobile remote-control platform provides consumers with tremendous flexibility with demand-side energy management. A smartphone can communicate via the internet with web servers and connect them with intelligent home management systems. To minimize the cost of use and maintain the existing appliances may be operated and controlled very easily at home anywhere and anytime with respect to Digital Construction of educational Contents [10].

[11]Evaluates the ironclads app allows a user to safely transfer their data to a distant machine, ensuring that every instruction on that every instruction of that machine follows the application's formal abstract behaviors. This eliminates the weaknesses in implementing them such as buffer overrun, parsing mistakes, or data leaks. It notifies the user program will always behave. These guarantees are provided by full, low-level verification tools. Then employ encryption and safe hardware to allow remote users secure pathways from the controlled software. Then create a new and amended toolbox, a set of approaches and disciplines, and a procedure for the quick verified production systems software to achieve such a verification. Thus discuss the process, official results, and lessons from constructing the entire software package that has been verified. This program consists of a validated system; kernel; drivers and crypto libraries that were verified, including the HMAC, RSA, and SHA and four ironclad apps.

[12] suggests a comprehensive safety plan for the internet of things enabled by mobility (IoT). A safe regime of the proposed scheme and i) efficient DTLS handshake-based end-user authentication and authorizing architecture, ii) safe end-to-end statement based on the restart of an assembly, and iii) robust smart gateways-based mobility. The plan is simulation demonstrated and a full prototype of hardware. Based on this scheme contains the most comprehensive security features in this analysis compare with comparable literature approaches. Energy-performance assessment results demonstrate that our strategy decreases overhead communication by 26% and delay of a statement between the smart gates and end-users by 16% as compared with a conventional approach. Additionally, this system is approximately 97% faster than the certificate-based system and 10% faster than the symmetrical key-based DTLS. DTLS uses about 2.2 times as much Ram and 2.9 times as many ROM resources as the method. RAM and ROM needs are nearly as low as the DTLS symmetric key. The solution analysis showed that mobility is low latency and that there is no dispensation or aerial communication of the sensors during the supply chain.

[13]introduced a safe and end-to-end secure, energy routing building in the IoT allows environmental health observation in integrated devices. That gives the patient and the physician convenience, because the physical occurrence of both is not required for medical monitoring. The new technology can be used in a variety of sectors, such as real-time patient health surveillance, patient maintenance, and distant health care. This new technological development without analysis, security, and energy consumption in the application of healthcare. The renders patient privacy, susceptible and also subject to environmental and operational damage. End-to-end safety and energetic routing procedures for its-based on the medical application are not assured by existing technologies.

[14]evaluates an intrusion detection system (IDS) survey is offered depending on the latest concepts and methodologies suggested for it. The survey begins with a historical study of the IDS to explain and illustrate the distinctions between the IDS platform and the current trend of research towards a universal and multiplatform method. A look at current holistic trends and an analysis of such diets are followed in this review of the fundamentals of IDS investigation into the components it. Finally, guidance on possible of IDS on the IoT is provided before the open research issues are identified.

3. Methodology

3.1. Global system for mobile communication (GSM)

GSM is a public phone service digital cellular scheme. It was created for a uniform European standard for mobile phones and was quickly accepted throughout the world. Currently, a new tendency for many different applications is the mobile phone system. GSM has been developed to be ISDN service compatible. It can thus be part of a telephone system together [15]. The GSM consists of three components: the Mobile Station (MS), the basic station subsystem (BSS), and the network subsystem (NS). The MS includes the mobile devices and Subscriber Identification Modules (SIMs).

Mobile device design such as the device or modem can change for different applications, depending on user specification. The key part of NS is the mobile switching service center (MSC). Other aspects of the NS have been specifically created to connect PSTN public switched telephone networks, public switched data networks (PSDNs), or the integrated digital service network (ISDN). As part of this router design, the proposed GSM real-time control system can be connected to any remote terminal. For digital data processing, GSM uses multi-access time allocation (TDMA). Two 45 MHz separate bands for GSM uplink and downlink operations were set up within the 900 MHz system. A single carrier channel of 200 kHz width is split into 124 each as 25 MHz bandwidth. The same is true for systems with 1800 and 1900 MHz in the basic transceiver station (BTS). The cell is composed of several of such frequency, channels called cell assignment. The frequency, channels of each 200 kHz bandwidth carry 8 TDMA channels, each dividing into eight-time slots. The TDMS channels are 8 times a frame for the TDMA channel [16]. The TDMA frame lasts 156.25-bit every time.

The time frame is about 15/26 ms or 576.9s, therefore a frame is 4.613 msin a one-time slot is described as a physical channel is a recurrence. A GSM MS with an upward and downward connection uses the same two locations. BTSs have been increased enormously to provide greater service quality. By cellular arrangement, service signals from one MS or user numerous BTSs in various directions [17]. Accessibility, availability, and reliability have improved greatly in terms of service quality. They can connect GSM services via a PPP (point-to-point protocol). Some of the MS is called the mobile user, and the other end may differ from another MS or telephone terminal. The proposed real-time GSM control structures in most applications can be boundless in such a service context [18]. With the GIS, visual basic (VB) connection mode under GIS map info the methodology based on the real-time control the idea setup can work on Microsoft Windows operating system MS platform as illustrated in Fig. 1.

3.2. Overview of Remote-control system

A device search is multiplied package to search for the ECHONET home network devices for ECHONET Lite controlling devices [19]. The devices sent the answer to the controller unicast when devices got the packet from ECHONET Lite. By receiving the response, ECHONET Lite devices are detected controllers in the home network. A control communication is sent to the detected device by the controller, and the device's ECHONET Lute control is carried out. The ECHONET home network devices cannot be found directly from the message from the device search is locally addressed. For the above-mentioned challenges, the manufacturer uses the system model used to build RCS servers in a remote control service overview, which is displayed in Fig. 2. This document is referred to as an RCS using a way for such an existing RCS.

The control did not send the search for the device defined directly to the controller by ECHONET Lite specification [20]. The controller uses web technologies such as HTTPS to reach the RCS server and sends a control message with manufacturing specifications. There are essentially two methods for passing device control messages to the home gateway (HGW) from the RCS server. One is to transfer the RCS server

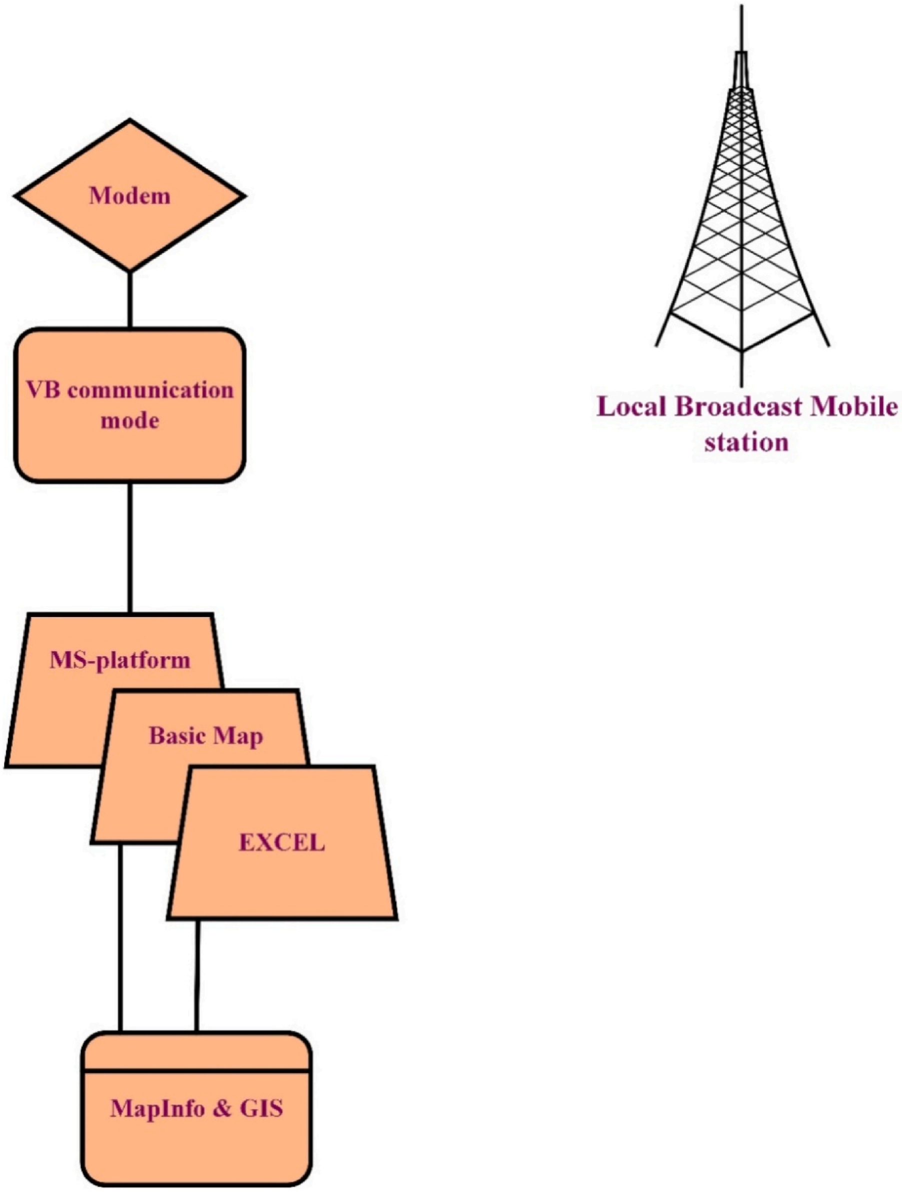

Fig. 1. Global system for real-time mobile system architecture.

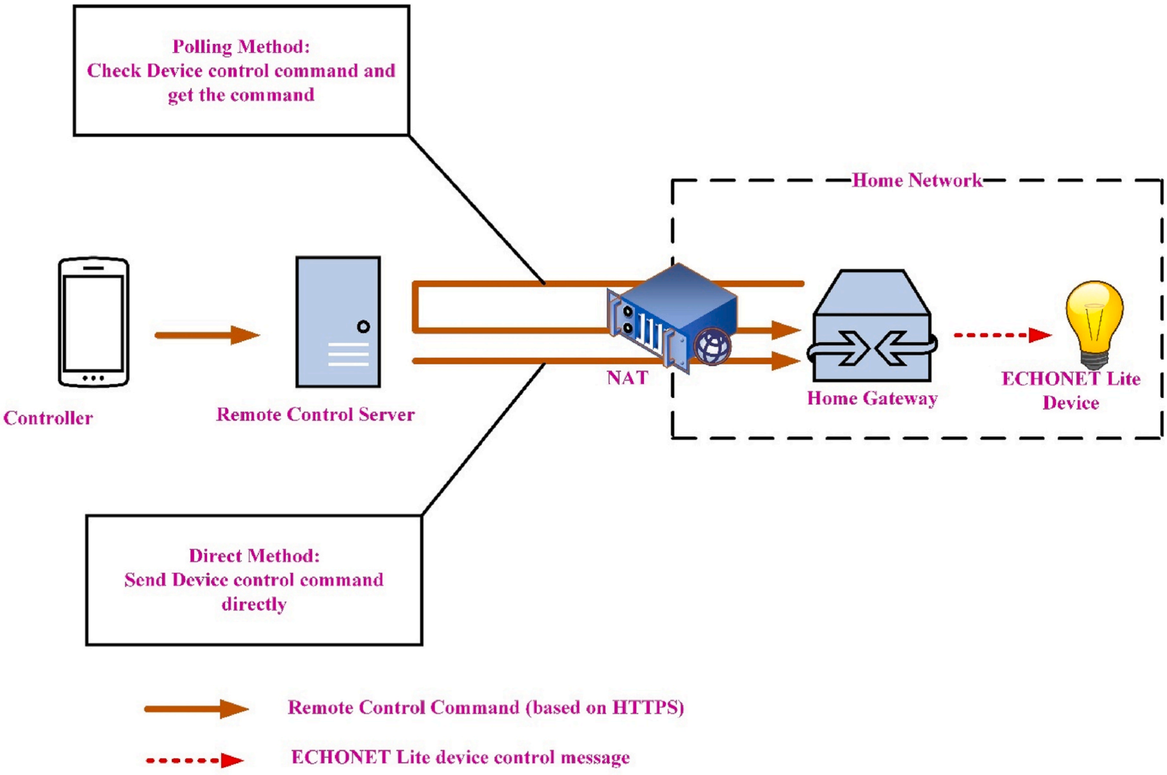
Polling Method:
Check Device control command and get the command
Home Network
Controller
Remote Control Server
NAT
Home Gateway
ECHONET Lite Device
Direct Method:
Send Device control command directly
Remote Control Command (based on HTTPS)
ECHONET Lite device control message

Fig. 2. Overview of Remote-control system.

messages directly by situation up transmission to the home network's wideband router. The alternative techniques are to periodically receive the device control messages from the HGW to the RCS server [21]. HGW accepts control messages and establishes communication with the ECHONET Lite returns the controller response message via the RCS server.

The method can receive a message from the unit control controls so that the user's operating history is obtained from the manufacturer. Therefore, when the RCS happens, the manufacturer may discover a log information reason. Furthermore, manufactures can find out what kind of devices the user controls, and manufacturers can create a new service and product development by analyzing the log information. However, the user will use if the user is the house ECHONET Lite-enabled (Controller app) [22]. But if the users are outside of the house, the user utilizes a web browser-like controller application. Thus, according to the location, the user must select the program. In addition, the company has controller two type applications supply and the service of remote-control to enhance the development costs, respectively. When the manufacturer terminates the RCS the user is could no longer work from outside all ECHONET Lite devices. The RCS must be operated permanently and continuously manufacturer's server [23]. Moreover, if a third party leaks the transaction history maintained on the RCS server, the privacy of the user may be violated. This results in the third party guessing the user's lifestyle and the aim to lead to privacy and crime violations.

3.3. System configuration

NT Mobile is an end-to-end communication architecture that, in IPV4/IPV6 networks can provide both connection and mobility. In the NT Mobile architecture, NTM nodes create a link that doesn't exist in real networks using its virtual IP addresses. Data packets are encrypted and transferred between the NTM nodes using the user datagram (UDP) based on virtual IP addresses [24]. Any NTM node applications can communicate without influencing NAT's existence within the communication connection. In Fig. 3 displays the system setup and remote-control, communication status of the proposed system. An extended NT Mobile ECHONET Lite controller deployed on a foreign network is a mobile node (MN).

A commercially available home appliance is an ECHONET Lite Device (ELD), which is obtainable on the house network. The newly specified home device implementing the planned scheme is a Remote-ControlAgent (RCA) with NTMobile expanded features, including virtual IP address allocations for the ELDs, on the Address Allocation Table (AAT) administration, NAT-Lite address for translation [25]. The MN establishes a UDP RCA tunnel in the direction of the DC on the internet and transmits the ELD virtual IP address message to the ECHONET Lite (VIPELD). The RCA decodes and uncovers incoming communications and transforms the address into the ELD IP address in question (RIPELD) based on AAT from the virtual IP address [26]. These communications can be transmitted mutually among the ELD and the MN without the need for a server supporting remote control.

In a UDP tunnel setup, the operation is launched with the packet detection for the DNS request as a trigger existing NTMobile architecture. The NTMobile will be expanded to initiate the tunnel with a search message for the methodology with an ECHONET Lite device is shown in Fig. 4. If a multicasts device search message is used by an ECHONET Lite application, the enhanced function NTMobile begins to create the RCA tunnel; A multicast request is forwarded towards the RCA by DC and support afterward [27].

The RCA generated a device search, message and connects it to the house network based on the multicast request from the recipient. Later receiving a multiple task message, the ELDs give the MN virtual IP address as a response message (VIPMN) [28]. The proposed system receives packets to the virtual IP address on behalf of the RCA. The RCA assigned the ELD's internally unused virtual IP address, which delivered the response message, and recorded both the virtual and actual IP addresses in the AAT. The RCA converts the response message's address of the source from the RIPELD to the VIPELD and sends it to the MN via the UDP tunnel. ECHONET Lite identifies the ECHONET Lite within the

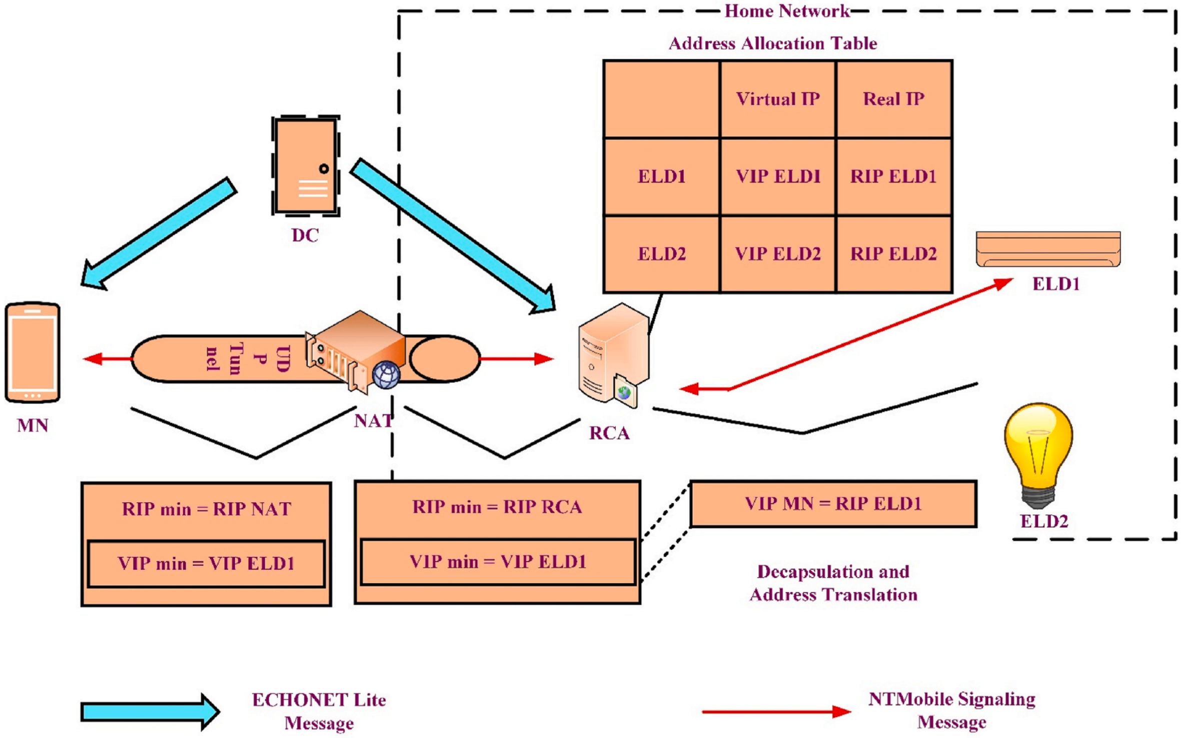

Fig. 3. Configuration of remote-control communication.

domestic network and identifies the IP addresses of the devices [29]. The MN transmits to VIPELD an ECHONET Lite control message, when controlling remotely the found equipment, leveraging a UDP tunnel set up during the search. The RCA decrypts the packet, which is subsequently transported to AAT based on VIPELD to RIPELD. The check message is sent to the ECHONET Lite device from the MN. The gadget processes, communication and responses are returned to the MN.

4. Implementation and evaluation

This can be implemented by expanding a regular NT Mobile prototype of the desired system. When the UDP tunnel is established by the NT Mobile signaling message is changed to the NTM tunnel request and Response. The NTM node can be transferred beyond NAT to the RCA by using the channel. The prototype implementation is given below for both MN and RCA.

4.1. Mobile node (MN)

The modular design of the MN is displayed in Fig. 5. Thus, have implemented MN via NTMobile type VPN service since MN is considered to be a regular mobile device. Using VPN service API to identify multicast device search messages expanded the module for determining packets and configuring routing tables [30]. After MN created a UDP tunnel to the default RCA when receiving the search device message, the NT Mobile tunnel service introduced a mechanism to submit a multi-cast request. Moreover, then used traditional NT Mobile as the device control message encryption and decryption feature.

4.2. Remote control agent (RCA)

The structure of the RCA module appears in Fig. 6. In combination with the usual RS and NTM node module, created the RCA daemon. Then created the RCA daemon, used by the RCA daemon function to build a multicast request-based device search message if a multicast request is received by the RCA daemon. In addition, net filters are a Linux standard NAT function that was created for the RCA address translation function [31]. Construct an AAT to maintain multiple virtual IP addresses and to dynamically assign all ECHONET lite devices a virtual IP address. Moreover, the RCA is the daemon of Routing Information Protocol (RIP) to receive the response message delivered by ELD on behalf of VIP_{MN}.

4.3. Configuration of network

Table 1 shows the specification of devices. The DC and the RS had set up a VPS (Virtual Private Server). With the application “Enepota” 3, the MN controller sent ECHNONET Lite compliant messages. The MN was a modern mobile phone, the RCA being mini-Linux [32]. The ELD is one air conditioning commercial room and the HGW has been installed behind the NAT router, inthe laboratory network. Then, timed the time to clarify the response time within the proposed system.

- Tunnel layout: Time required from MN to RCA for the tunnel.
- An exploration development for the devices: The time necessary to obtain a response from the air conditioner since the beginning of the research by the MN ECHONET Lite devices.
- Device Controller Process: The time to receive a response from the air conditioner from delivering an air conditioner control message.

Next, look at the packet’s transmit time by identifying the ratio in between the timestamps just before and after the packets are transmitted and received. By the way, the controlled air conditioner had the power OFF status(X [33]. Table 2 presents the proposed system climate control system 50 times per treatment period. The processes were confirmed in a short period, with an average focus. The tunnel setting process is the first time the device search is sent or the MN moves to another network.

Then, the timeout until receipt of defining the response message of the control message transmission following the ECHONET Lite specification as 5000 ms Thus. The overall effect of the system proposed does not affect communication with ECHONET Lite and it has been observed that the actual mobile internet as well as environment functions.

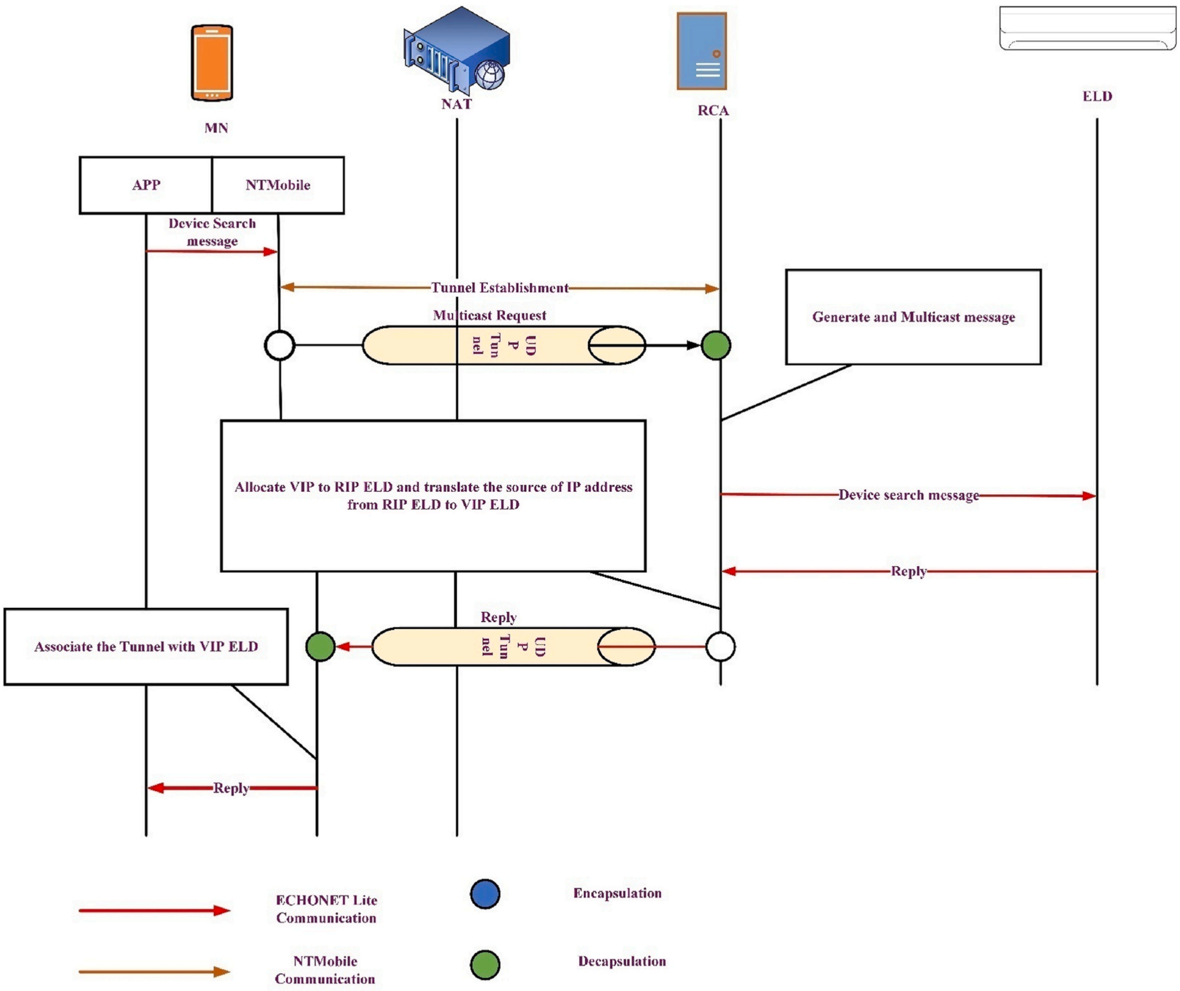

Fig. 4. ECHONET Lite search device sequence.

4.4. Quantitative evaluation

Users can't control from the outside once the RCS server is down or the intrusion detection service is terminated completely, there is a comparable problem in a location number. Problems like the current system are not directly reported in the proposed system controller and the RCA [34] The user can also use an app and the user has no place to change an application. The applications outside the house need not be developed by the producers. The servers to be utilized in the planned system can be generally employed in the NTMobile communication, but can also be used other than the remote-control applications.

A pair of the response packages and control packages, devices have been difficult to identify completely since the existing service communicates with HTTPS. The time to respond by packing cannot be estimated. Therefore, by capturing video of a device control with each approach, determined the needed time for the control as the time difference from the start of the controller in response to the air conditioner. As a video camera can use the android modern smartphone, the file is 30fps image rate and the format is MP4 [35]. The results of the system proposed are already established by the MN and RCA state tunnel state, however, Table 2 results of the tunneling were completed by around 1 s on average. The system proposed was determined to be equivalent to or greater than the existing service performance in comparison to the two. In addition, the processing time for the system devices was estimated by deducting the RTT from the average time of each method control device [36]. As a result, 503 ms were taken from the system and 1486 ms from the current service. This shows that the current service has more processing time than the system proposed. Then found that it's because, in existing services, the remote control server and HGW processing time is more than the system proposed.

Therefore, a dedicated server such as the remote control present system is no longer required by the fabricator to design and manage. This means that the suggested system will not be affected and can be stated to be better in terms of privacy by the user's unmanaged devices and services [37]. User authentication is among the remote control security features. It introduces a way to authenticate the user at the start of the communication the foundation of the proposed system in the NTMobile. If the authentication fails, NTMobile's communication method can't be carried out itself.

Additionally, the RCA can easily determine that the RCA enables tunnel creation and tunnel communication only with a certain NTM node by implementing the access control function in the RCA and denies communication from the other devices. By the way, VPN is typical of the way a controller accesses a gadget remotely on the home network [38]. Technically, it is feasible to remotely control ECHONET Lite devices with a VPN. However, for transmission of multicast packets related to the device search, it must be typed into a sub-network of L2-VPN. Even L3-VPN must be supported for multicast routing. If a virtual VPN is used, the manufacturers can access a device other than ECHONET Lite if they offer a service such as remote diagnosis and remote diagnostic [39]. On the other hand, since the system allows the remote-control only for the ECHONET Lite device's session, the system Presented is safe.

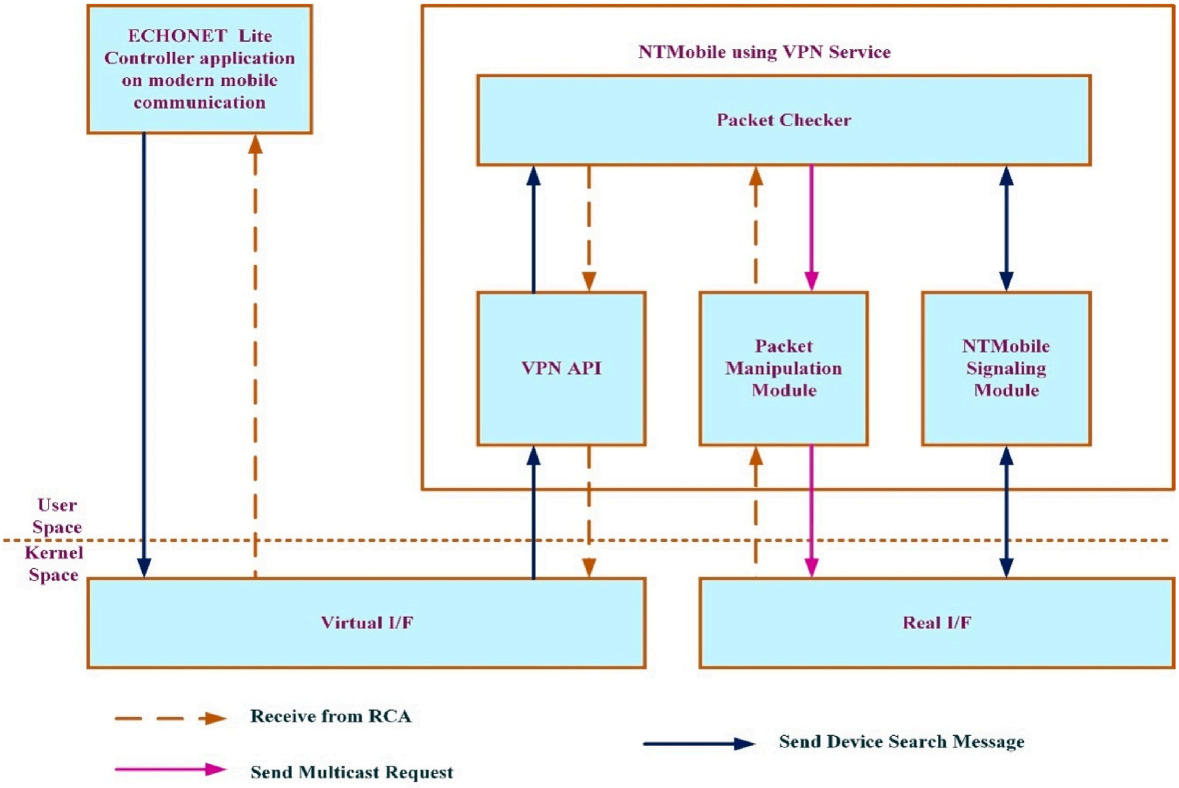
ECHONET Lite Controller application on modern mobile communication
NTMobile using VPN Service
Packet Checker
VPN API
Packet Manipulation Module
NTMobile Signaling Module
User Space
Kernel Space
Virtual I/F
Real I/F
Receive from RCA
Send Device Search Message
Send Multicast Request

Fig. 5. Structure module of Mobile Node (MN).

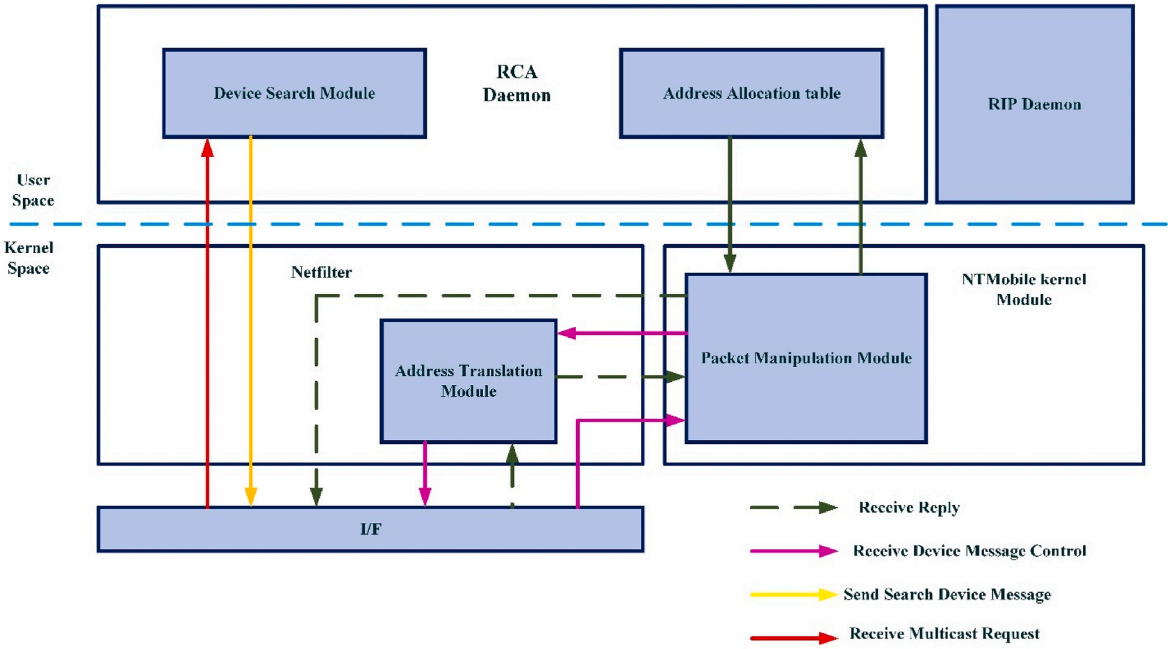
Device Search Module
RCA Daemon
Address Allocation table
RIP Daemon
User Space
Kernel Space
Netfilter
NTMobile kernel Module
Address Translation Module
Packet Manipulation Module
I/F
Receive Reply
Receive Device Message Control
Send Search Device Message
Receive Multicast Request

Fig. 6. Structure module of RCA

5. Conclusion

This study, assessed and confirmed the achievement of end-to-end security with a remote-control system using a modern mobile communication on ECHONET Lite device. Then check the current mobile internet environment works and evaluated its performance. As a result, the proposed solution has been proven as being capable of controlling ECHONET Lite devices without the usage of a specific server, at the same network performance as a traditional remote control system. The proposed technology was aimed to convert non-ECHONET lite protocols. In the control of ECHONET, all the internet messages are encrypted and the server does not preserve operational history. A secure and reliable remote control system therefore they can be established that protects the user's privacy.

Table 1
Specification of devices.

	CPU	Memory
MN	Snapdragon 820 2.25 GHZ	3 GB
RCA	Intel Celeron N2830 2.16 GHz	8 GB
DC	Virtual CPU 1 core 3.3 GHz	512 MB
RS	Virtual CPU 2 Core 3.1 GHz	1536 MB

Table 2
Each communication process response time.

	Min [ms]	Avg [ms]	Max [ms]
Tunnel establishment	615.13	1061.00	1727.67
Discovery Device	86.66	460.75	1151.47
Device Control	65.31	316.60	1221.12

CRediT authorship contribution statement

D. Venu: Conceptualization, Methodology. **Babu J:** Data Collection related to Mobile Computing, Data curation. **R. Saravanakumar:** Remote control system Concepts drafting, Writing – original draft. **Ricardo Fernando Cosio Borda:** Implementation and, Validation. **Yousef Methkal Abd Algani:** Additional, Validation. **B. Kiran Bala:** Overall, Supervision.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

References

[1] Hae-Duck Jeong, Sang-Kug Ye, Jiyoung Lim, Ilsun You, Wooseok Hyun, A computer remote control system based on speech recognition technologies of mobile devices and wireless communication technologies, Comput. Sci. Inf. Syst. 11 (3) (2014) 1001–1016, https://doi.org/10.2298/CSIS130915061J.

[2] Hisayoshi Tanaka, Hidekazu Suzuki, Akira Watanabe, Katsuhiro Naito, Proposal for a secure end-to-end remote control system for ECHONET lite home appliances, in: 2017 IEEE 6th Global Conference on Consumer Electronics (GCCE), 1–2, IEEE, Nagoya, 2017, https://doi.org/10.1109/GCCE.2017.8229360.

[3] Daniel Hess, Christof Rohrig, Remote controlling of technical systems using mobile devices, in: 2009 IEEE International Workshop on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications, vols. 625–28, IEEE, Rende, 2009, https://doi.org/10.1109/IDAACS.2009.5342900.

[4] Thomas Kobzan, Sebastian Schriegel, Althoff Simon, Boschmann Alexander, Jens Otto, Jorgen Jasperneite, Secure and time-sensitive communication for remote process control and monitoring, in: *2018 IEEE 23rd International Conference On Emerging Technologies And Factory Automation (ETFA)*, 1105–8, IEEE, Turin, Italy, 2018, https://doi.org/10.1109/ETFA.2018.8502539.

[5] Arbab Waheed Ahmad, Naeem Jan, Saeed Iqbal, Chankil Lee, Implementation of ZigBee-GSM based home security monitoring and remote control system, in: *2011 IEEE 54th International Midwest Symposium On Circuits And Systems (MWSCAS)*, 1–4, IEEE, Seoul, Korea (South), 2011, https://doi.org/10.1109/MWSCAS.2011.6026611.

[6] Hisayoshi Tanaka, Hidekazu Suzuki, Naito Katsuhiro, Akira Watanabe, Implementation of secure end-to-end remote control system for smart home appliances on android (ICCE 2019 report), ITE Tech. Rep. 43 (5) (2019) 27–32.

[7] Hidekazu Suzuki, Katsuhiro Naito, Kazuma Kamienoo, Tatsuya Hirose, Akira Watanabe, Ntmobile: new end-to-end communication architecture in Ipv4 and Ipv6 networks, in: Proceedings of the 19th Annual International Conference on Mobile Computing & Networking, 2013, pp. 171–174.

[8] Hiroyuki Fujita, Hiroshi Sugimura, Moe Hamamoto, Masao Isshiki, Improvement of the device descriptions of echonet lite by adding version specific information, in: 2019 IEEE 8th Global Conference on Consumer Electronics (GCCE), 791–93, IEEE, 2019.

[9] En Qing Ji, Hai Gang Shi, Hong Yi Li, Qian Tang, Research on new remote control platform for smart home system using mobile phones, Appl. Mech. Mater. 473 (December) (2013) 267–274. https://doi.org/10.4028/www.scientific.net/AMM.473.267.

[10] Zhu Hong, Edge computing in mobile information system for digital construction of college\ English teaching, Wireless Commun. Mobile Comput. 2021 (2021), https://doi.org/10.1155/2021/6946454. Article ID 6946454, 15 pages.

[11] Hawblitzel, Chris, Jon Howell, Jacob R Lorch, Arjun Narayan, Bryan Parno, Danfeng Zhang, and Brian Zill. n.d. "Ironclad Apps: End-To-End Security via Automated Full-System Verification," vol. 18.

[12] Moosavi, Sanaz Rahimi, Tuan Nguyen Gia, Ethiopia Nigussie, Amir M. Rahmani, Seppo Virtanen, Hannu Tenhunen, Jouni Isoaho, End-to-End security scheme for mobility enabled healthcare internet of things, Future Generat. Comput. Syst. 64 (November) (2016) 108–124, https://doi.org/10.1016/j.future.2016.02.020.

[13] R. Nidhya, S. Karthik, G. Smilarubavathy, An end-to-end secure and energy-aware routing mechanism for IoT-based modern health care system, in: Jiacun Wang, G. Ram Mohana Reddy, V. Kamakshi Prasad, V. Sivakumar Reddy (Eds.), Soft Computing and Signal Processing, 2019, https://doi.org/10.1007/978-981-13-3600-3_35, 900:379–88. Advances in Intelligent Systems and Computing. Singapore: Springer Singapore.

[14] Gendreau, A. Audrey, Moorman Michael, Survey of intrusion detection systems towards an end to end secure internet of things, in: 2016 IEEE 4th International Conference on Future Internet of Things and Cloud (FiCloud), vols. 84–90, IEEE, Vienna, Austria, 2016, https://doi.org/10.1109/FiCloud.2016.20.

[15] Guifen Gu, Guili Peng, The survey of GSM wireless communication system, in: 2010 International Conference on Computer and Information Application, IEEE, 2010, pp. 121–124.

[16] Jain Cai, David J. Goodman, General packet radio service in GSM, IEEE Commun. Mag. 35 (10) (1997) 122–131.

[17] Mohammad Asif Habibi, Meysam Nasimi, Bin Han, Hans D. Schotten, A comprehensive survey of RAN architectures toward 5G mobile communication system, IEEE Access 7 (2019) 70371–70421.

[18] Bidwai, SS, VB Kumbhar, and Mr AR Nichal. n.d. "Real time automated control using PLC-VB communication." Int. J. Eng. Res. Afr. *Vol* 3: 658–661.

[19] Shohei Saito, Norihiro Ishikawa, Yosuke Tsuchiya, Development of echonet lite-compliant home appliances control system using pucc protocols from smart devices, in: 2015 IEEE 39th Annual Computer Software and Applications Conference, 3:200–204, IEEE, 2015.

[20] Takashi Murakami, Hiroshi Sugimura, Masao Isshiki, Application of ECHONET lite which is open standard into energy management system, in: 2016 IEEE International Conference on Consumer Electronics (ICCE), 455–58, IEEE, 2016.

[21] Rose Qingyang Hu, Jeff Babbitt, Hosame Abu-Amara, Catherine Rosenberg, G. Lazarou, Connectivity planning and call admission control in an on-board cross-connect based multimedia GEO satellite network, in: IEEE International Conference on Communications, 2003. ICC'03, vol. 1, IEEE, 2003, pp. 422–427.

[22] Akira Utakouji, Taeko Nakamura, Tatsuya Ozawa, Certification and test for radio comunication system in internet of things (IoT) and future prospects, IEICE Tech. Rep. 115 (474) (2016), 99–99.

[23] Yarali, Abdulrahman, Manu Srinath, and Randal G Joyce. n.d. "A Study of Various Network Security Challenges in the Internet of Things (IoT).".

[24] Kazuma Kamienoo, Hidekazu Suzuki, Katsuhiro Naito, Akira Watanabe, Development of mobile communication framework based on NTMobile, in: 2014 Seventh International Conference on Mobile Computing and Ubiquitous Networking (ICMU), 27–32, IEEE, 2014.

[25] Katsuhiro Naito, Takuya Nishio, Kazuo Mori, Hideo Kobayashi, Kazuma Kamienoo, Hidekazu Suzuki, Akira Watanabe, Proposal of seamless ip mobility schemes: network traversal with mobility (ntmobile), in: 2012 IEEE Global Communications Conference (GLOBECOM), 2572–77, IEEE, 2012.

[26] Yuya Miyazaki, Fumihito Sugihara, Katsuhiro Naito, Hidekazu Suzuki, Akira Watanabe, Certificate based key exchange scheme for encrypted communication in NTMobile networks, in: Proceedings of the 12th IEEE VTS Asia Pacific Wireless Communications Symposium, APWCS, 2015, pp. 1–5.

[27] Kaito Kuromiya, Hisayoshi Tanaka, Hidekazu Suzuki, Katsuhiro Naito, Akira Watanabe, Implementation and evaluation of IP mobility functions in NTMobile for android, in: 2018 Eleventh International Conference on Mobile Computing and Ubiquitous Network (ICMU), 1–4, IEEE, 2018.

[28] Li Fengjun, Zhenjiang Dong, Hongwei Wang, Message service system evolution and general frameworks, ZTE Commun. 7 (3) (2020) 49–53.

[29] Peter Curwen, Jason Whalley, Mobile Telecommunications Networks: Restructuring as a Response to a Challenging Environment, Edward Elgar Publishing, 2014.

[30] Jose Polo, Gemma Hornero, Coen Duijneveld, Alberto García, Oscar Casas, Design of a low-cost wireless sensor network with UAV mobile node for agricultural applications, Comput. Electron. Agric. 119 (2015) 19–32.

[31] Gabriel Villarrubia, Juan F. De Paz, Javier Bajo, Juan M. Corchado, Ambient agents: embedded agents for remote control and monitoring using the PANGEA platform, Sensors 14 (8) (2014) 13955–13979.

[32] Andres Kwasinski, Alexis Kwasinski, Architecture for green mobile network powered from renewable energy in microgrid configuration, in: 2013 IEEE Wireless Communications and Networking Conference (WCNC), 1273–78, IEEE, 2013.

[33] Xiaonan Wang, Huanyan Qian, Dynamic and hierarchical IPv6 address configuration for a mobile ad hoc network, Int. J. Commun. Syst. 28 (1) (2015) 127–146.

[34] Mohammad Jafari, Alireza Mohammad Shahri, Seyyed Hamid Elyas, Optimal tuning of brain emotional learning based intelligent controller using clonal selection algorithm, in: ICCKE 2013, IEEE, 2013, pp. 30–34.

[35] M. Shafei, M. Rezaei, S. Tavakoli, F. MohannaA, Fuzzy video rate controller for variable bit rate applications using ANFIS, in: International Conference on Communications Engineering (ICComE 2010), vol. 22, 2010.

[36] Daniel Granlund, Christer AAhlund, A scalability study of AAA support in heterogeneous networking environments with global roaming support, in: 2011IEEE 10th International Conference on Trust, Security and Privacy in Computing and Communications, vols. 488–93, IEEE, 2011.

[37] Juliana Sutanto, Elia Palme, Chuan-Hoo Tan, Chee Wei Phang, Addressing the personalization-privacy paradox: an empirical assessment from a field experiment on smartphone users, MIS Q. (2013) 1141–1164.

[38] Y.P. Kosta, Upena D Dalal, Rakesh Kumar Jha, Security comparison of wired and wireless network with firewall and virtual private network (VPN), in: 2010 International Conference on Recent Trends in Information, Telecommunication and Computing, 281–83, IEEE, 2010.

[39] Roşu, Marius Sebastian, Drăgoi George, VPN solutions and network monitoring to support virtual teams work in virtual enterprises, Comput. Sci. Inf. Syst. 8 (1) (2011) 1–26.