Privacy and safety of narrowband internet of things devices

Ali Abdollahi[1], Shohreh Behnam Arzandeh[2], Mohsen Sheibani[3]
[1]Information Technology Researcher, Randstad, Netherlands
[2]Department of Infomration, Technology Management, SRBIAU, Tehran, Iran
[3]Faculty of Computer Engineering, Najafabad Branch, Islamic Azad University, Najafabad, Iran

Article Info

Article history:

Received Mar 10, 2021
Revised Feb 10, 2024
Accepted Mar 29, 2024

Keywords:

Internet of things;
Long-term evolution;
Narrowband internet of things;
Privacy;
Telecommunication;

ABSTRACT

Technology's increasing role in everyday life has pushed the evolution of the internet of things (IoT), which now permeates industries like information technology, agribusiness, and transportation. Critical concerns in IoT security include platform diversity and issues with authentication and authorization. Critical vulnerabilities identified by researchers contain unencrypted communications, compromised interfaces, and compromised access control processes. A new solution, narrowband IoT (NB-IoT), has responded. Based on the cellular network, this technology is designed for improved security and efficiency, operating within the fourth-generation mobile networks and leveraging essential network components. The current study focuses on NB-IoT vulnerabilities, particularly in the radio segment, which is notably vulnerable. The research utilized the open-source tool OpenLTE and hardware like software-defined radio (SDR) in a setting with active NB-IoT sensors on an LTE network. This included deploying a test listening tool and a laboratory-based IMSI catcher to intercept active device communications in a testbed. The results highlight significant vulnerabilities: sensors were deactivated following simulated network attacks with rogue eNodeB and traffic area update (TAU) messages, revealing the technology's susceptibility to connection failure.

Corresponding Author:

Ali Abdollahi
Information Technology Researcher
Randstad, Netherlands
Email: ali.abdollahi19@gmail.com

1. INTRODUCTION

The internet of things (IoT) offers a vision of the Internet of the future as users, computing systems, and everyday objects with sensing and operating capabilities collaborate with unprecedented advantages and economic benefits [1]. One of the most important IoT challenges is security, where attacks such as Sinkhole and Clone ID can occur in the IoT network, leading to other attacks, including Eavesdropping [2]. Eavesdropping is one of the main privacy issues which is considered in the presented article. the hackers could actually use a connected device to IoT networks to virtually invade a person's privacy. Given that security is the main factor in the connection of applications in the IoT, mechanisms should also be designed based on security. The IoT contributes to advanced applications and new business openings in worldwide parts, for example, the fourth industrial revolution (Industry 4.0) and smart cities and precision agriculture, among others [3]. Having every 'thing' associated with the worldwide future IoT communicating with one another, new security and protection issues emerge, e.g., privacy, integrity, and authenticity of data discovered and exchanged by 'things' [4].

Ongoing IoT technologies (e.g., narrowband IoT (NB-IoT) [5], long-range wide-area network (LoRaWAN) [6], and Sigfox [7], like low power WANs (LPWANs) offer long-go interchanges and decreased energy costs, which advances the formation of new IoT applications and administrations in Industry 4.0 [8].

With the growth and improvement of the IoT network and the arrival of various devices and the need to connect them, by 2030 we will see the integration of 125 billion devices with various structures in this network. However, many of these devices are deployed without considering the security; therefore, such connectivity causes a new range of security risks [9]. The wide spreading of IoT technologies have prompted the ascent of LPWAN solutions. Older cellular technologies like 2G/3G/4G networks expend an excess of power. In addition, they do not fit well with applications where just a modest quantity of information is communicated rarely. Cellular IoT is trying to react to the endless quest for better long-range, low-power applications. LPWA networks offer a new class of wireless infrastructure specifically developed for low-data IoT applications. The LPWAN is developed for IoT applications with low bandwidth, low power usage, long distance, and a large number of connections. NB-IoT, which supports data speed of up to 65 kps and is optimal for straightforward static sensor applications [10]. NB-IoT provides better performance when we equate NB-IoT's inherent capabilities with other LPWA technologies, such as electronic monitoring tourism controlling (e-MTC), SigFox, and LoRa. Moreover, when looking at all the technologies in terms of network capital spending, coverage circumstance, uplink and downlink traffic and network efficiency, we acknowledge that NB-IoT is the most powerful technology [11]. Due to its specifications of high energy consumption and long battery life, the NB-IoT is becoming a reliable approach for manufacturers of smart devices [12]. NB-IoT has a fairly comprehensive ecosystem, largely due to its sponsorship from many of the world's largest operators. Unlicensed solutions do not guarantee reliability and security, most importantly [11]. As a consequence, on 2G, 3G, and 4G networks it will coincide with appliances [13]. While we discuss about the IoT, cybersecurity is one of the aspects that most concerns users. There is also a consumer question about how to deal with the privacy and security of data produced by these devices. Within a NB-IoT network, the data will be in a more secure way rather than a simple IoT environment. The information challenges arise as soon as the data exits the NB-IoT network and is transmitted over the Internet from the network operator's servers to the final cloud server where its retrieval center and data analysis have been installed by the user. User datagram protocol (UDP) protocol is frequently used by the NB-IoT [14].

2. THEORICAL BASIS

Mobile operators use dedicated spectrum bands under the provisions of the licenses granted by their national regulators. The mobile operator members of the global system for mobile communications association (GSMA) provide connectivity using standardized network technologies, such as global system for mobile (GSM), universal mobile telecommunications system (UMTS), and long-term evolution (LTE), as specified by standards body 3rd generation partnership project (3GPP). The two major mobile IoT technologies, LTE-M and NB-IoT, standardized by 3GPP, are funded by large numbers of mobile operators and suppliers of equipment, allowing the ecosystem to benefit from economies of scale and low costs of development and deployment [15].

The security specifications of NB-IoT are close to those of standard IoT, but there are several variations, primarily with regard to low-energy IoT hardware, network connectivity mode and actual service specifications. The conventional IoT terminal device typically has powerful processing capacity, a complex network communication protocol, and a tighter security reinforcement strategy; typically, power consumption is high, and regular charging is important. Low-power IoT systems, on the other hand, are distinguished by low power consumption , low processing power, and non-frequent charging, which often suggests that security vulnerabilities are more likely to pose a threat to terminals. Moreover, the state of denial of service (DoS) may be triggered by basic resource use. In comparison, the number of low-power consumption IoT terminal systems is much higher in real implementation than in conventional IoT. As a consequence, even greater security incidents will result from some minor security risk [16]. NB-IoT is a centralized system such as LTE, where eNodeB manages both downlink and uplink scheduling to ensure the synchronization of resources between systems [17].

One of the key components for the implementation of machine to machine (M2M) networking systems and the dissemination of the IoT is considered to be LTE networks. As an opportunist for advanced communications networks with a subscription count in the billions, cybersecurity is of significant importance in LTE [18]. Security researchers can impersonate cell phone users by leveraging a flaw in the mobile communication protocol LTE. Therefore, through the cell phone bill, they will book fee-based services under their name that are paid for. "For example, an attacker may book facilities, stream screens, but the owner of the attacked phone would have to pay for them," according to the researcher, the flaw can also impact law enforcement agency inquiries because attackers may not only make payments on behalf of the victim but may also access websites using the name of the victim. The identified weakness affects all devices that communicate with LTE, i.e., nearly all mobile phones, laptops, and certain wired household appliances [19].

3. METHOD

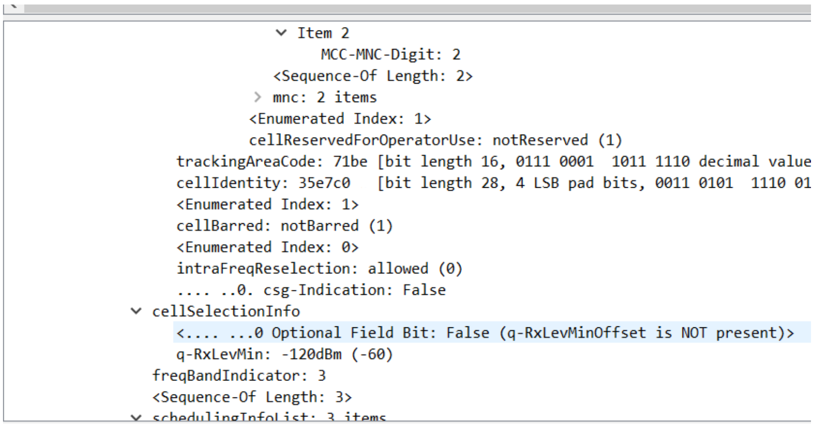
Due to the existence of vulnerabilities and extensive security holes in the GSM protocol, special efforts were made to improve privacy and design authentication processes in mobile networks, so the design and implementation of these algorithms in 3rd and 4th generations has been greatly improved. There is an advanced mutual authentication mechanism and encryption in the fourth generation. This has reduced security risk, but it should be noted that security concerns have not yet been fully addressed. Reasons for this include the vulnerability of this technology to attacks such as location tracking, fake eNodeB implementation or rogue eNodeB using protocol exploitation.

Based on the research and experiments performed in this study, which was performed on real networks, the LTE protocol in the access layer has vulnerabilities. In this study, data were analyzed using radio capture in LTE evolved UMTS terrestrial radio access network (E-UTRAN) without any special access. This protocol, despite security mechanisms such as encryption and mutual authentication, is vulnerable to protocol exploitation and setup rogue eNodeB (fake base station). An attacker can use this to eavesdrop on traffic with a SIM-Card or software-defined radio (SDR) [20].

This manuscript, inspired by this LTE protocol vulnerability justification, examines numerous areas of mobile network defense using low-cost radio device tools. A number of exploits are illustrated and introduced based on an open source version of the LTE stack, OpenLTE [21]. Mainly focused on the LTE stack's open source implementation, analysis is given on the growth of low-cost international mobile subscriber identity (IMSI) catchers and exploits that trigger blocking of mobile devices, which were first introduced globally in [22].

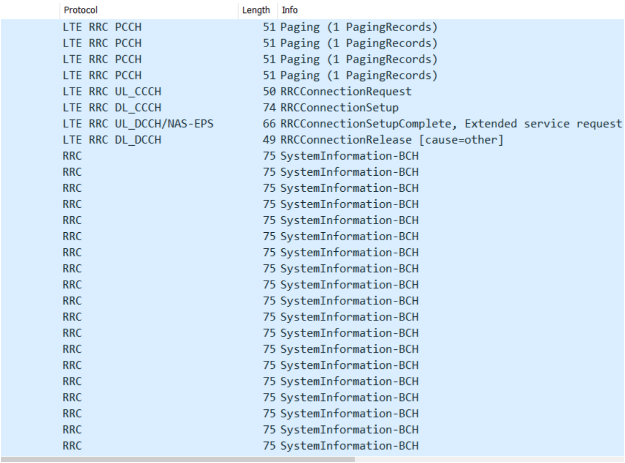
All the traffic and data collected in this study was captured by universal software radio peripheral (USRP) B210 and baseband [23], [24] by using these features, we will be able to capture and analyze data at the physical layer, such as receiving real-time information and decoding the non-access stratum (NAS), radio resource control (RRC) protocol, and system messages. The information gathered during the experiment is collected from a real and dynamic environment in an urban. In this active experiment, the sniffer system acted as an IMSI catcher and captured the IMSIs of active subscribers in that area. This analysis was performed with OpenLTE and srsLTE software in order to listen to traffic and implement eNodeB simultaneously [25]. All data exchanged between the user equipment (UE) tand the base-station is intercepted, but only control plane traffic that includes signaling data is important to us. This section examines the exploitation of the LTE protocol using the analysis of the collected signaling data.

Accordingly, a number of security aspects and abuse of the LTE protocol are presented, the most prominent of which are the extraction of information from system information block (SIB) and master (MIB) messages [26] and the DoS or DoS and location tracking using the implementation of rogue eNodeB. This simplifies the UE's initial access protocol, but could potentially be leveraged by an attacker to create sophisticated jamming attacks, customize the configuration of a rogue base station, or tuning other sophisticated attack types [27]. Figures 1 and 2 show an example of the contents of MIB and SIB1 messages in Wireshark transmitted by a commercial eNodeB in an area. From the information extracted from these messages, an attacker can discover the mobile operator that operates that cell, the tracking area code, received power threshold to trigger a handoff to an adjacent cell and a series of configuration data that could be influenced to setup a fake base station.



```
                 ⌄ Item 2
                      MCC-MNC-Digit: 2
                 <Sequence-Of Length: 2>
               › mnc: 2 items
              <Enumerated Index: 1>
              cellReservedForOperatorUse: notReserved (1)
      trackingAreaCode: 71be [bit length 16, 0111 0001  1011 1110 decimal value
      cellIdentity: 35e7c0   [bit length 28, 4 LSB pad bits, 0011 0101  1110 01
      <Enumerated Index: 1>
      cellBarred: notBarred (1)
      <Enumerated Index: 0>
      intraFreqReselection: allowed (0)
      .... ..0. csg-Indication: False
 ⌄ cellSelectionInfo
      <.... ...0 Optional Field Bit: False (q-RxLevMinOffset is NOT present)>
      q-RxLevMin: -120dBm (-60)
   freqBandIndicator: 3
   <Sequence-Of Length: 3>
 ⌄ schedulingInfoList: 3 items
```

Figure 1. Contents of MIB and SIB messages



```
Protocol                     Length  Info
LTE RRC PCCH                     51 Paging (1 PagingRecords)
LTE RRC PCCH                     51 Paging (1 PagingRecords)
LTE RRC PCCH                     51 Paging (1 PagingRecords)
LTE RRC PCCH                     51 Paging (1 PagingRecords)
LTE RRC UL_CCCH                  50 RRCConnectionRequest
LTE RRC DL_CCCH                  74 RRCConnectionSetup
LTE RRC UL_DCCH/NAS-EPS          66 RRCConnectionSetupComplete, Extended service request
LTE RRC DL_DCCH                  49 RRCConnectionRelease [cause=other]
RRC                              75 SystemInformation-BCH
RRC                              75 SystemInformation-BCH
RRC                              75 SystemInformation-BCH
RRC                              75 SystemInformation-BCH
RRC                              75 SystemInformation-BCH
RRC                              75 SystemInformation-BCH
RRC                              75 SystemInformation-BCH
RRC                              75 SystemInformation-BCH
RRC                              75 SystemInformation-BCH
RRC                              75 SystemInformation-BCH
RRC                              75 SystemInformation-BCH
RRC                              75 SystemInformation-BCH
RRC                              75 SystemInformation-BCH
RRC                              75 SystemInformation-BCH
RRC                              75 SystemInformation-BCH
RRC                              75 SystemInformation-BCH
RRC                              75 SystemInformation-BCH
RRC                              75 SystemInformation-BCH
RRC                              75 SystemInformation-BCH
```

Figure 2. Information from SIB and MIB messages in Wireshark

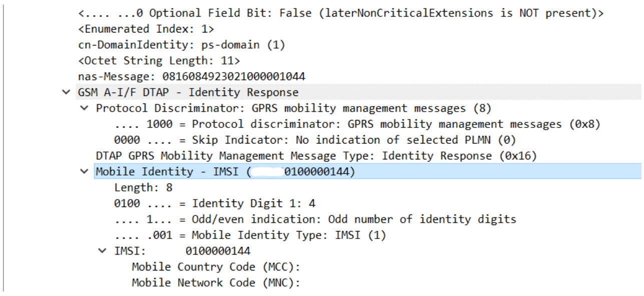
One of the most valuable segments of information, from a protocol exploit perspective, is the list of high priority frequencies. These parameters can be configured on a rogue eNodeB to activate most UEs to attach to it. Moreover, an attacker can also extract the mapping of important control channels on the PHY layer from the SIB messages. This can be leveraged to configure a smart jammer [28].

OpenLTE offers a traffic log feature for passively scanning broadcast information from nearby eNodeBs. A cost-effective option involves using an RTL-SDR radio with LTE cell scanner tool [29]. To done this research aims such as cell scanning and decoding SIB and MIB messages, all analysis including packet capturing have been done using crafted scripts and version of OpenLTE. The shots, depict neighbor cells that successfully detected by the tool. The decoded information of both MIB and SIB messages.

3.1. LTE-based imsi catcher

When the mobile device is turned on, it tries to connect to the network, and for authentication, it needs a unique identifier called IMSI, which is used for authentication on the network. A temporary mobile subscriber identity (TMSI) is derived until the device connects to an LTE network and can be used afterwards to keep the IMSI secret [30]. In order to implement and exploit this attack, it is necessary to capture subscriber's IMSI on air. The point here is that the low volume of IMSI values is exchanged between UEs and the network due to its very high importance. Sometimes this exchange supervenes under some situations. As when the subscriber intends to connect to the network, at that stage the UE sends the IMSI before authentication and NAS protocol processes. Now, the attacker disconnects the subscribers and implements rogue eNodeB so that all subscribers in that area send their IMSI numbers toward the attacker station.

A rogue eNodeB is a fake base station that is illegally set up on the LTE network and operated by an attacker via various open-source software frameworks, which are widely available [31]. As Figure 3 depicts a simple subscriber attach request in Wireshark, the subscriber has sent "Attach Request" message along with related IMSI value in clear-text to authenticate and complete the connection process to the network. If the rogue eNodeB has been set up with the required eNodeB network parameters, an attacker can now launch potentially serious threats such as man-in-the-middle (MITM) attacks, DoS, add malicious messages to the attachment process, deny UEs mobile services and downgrade to a non-LTE network. Moreover, DoS attacks that may lead to network failure are downgrading to a non-LTE network or refusing all network access [32].



```
    <.... ...0 Optional Field Bit: False (laterNonCriticalExtensions is NOT present)>
    <Enumerated Index: 1>
    cn-DomainIdentity: ps-domain (1)
    <Octet String Length: 11>
    nas-Message: 0816084923021000001044
  ⌄ GSM A-I/F DTAP - Identity Response
    ⌄ Protocol Discriminator: GPRS mobility management messages (8)
        .... 1000 = Protocol discriminator: GPRS mobility management messages (0x8)
        0000 .... = Skip Indicator: No indication of selected PLMN (0)
      DTAP GPRS Mobility Management Message Type: Identity Response (0x16)
    ⌄ Mobile Identity - IMSI (      0100000144)
        Length: 8
        0100 .... = Identity Digit 1: 4
        .... 1... = Odd/even indication: Odd number of identity digits
        .... .001 = Mobile Identity Type: IMSI (1)
      ⌄ IMSI:      0100000144
          Mobile Country Code (MCC):
          Mobile Network Code (MNC):
```

Figure 3. Attach request was sent along with IMSI

4. RESULTS AND DISCUSSION

Protocol exploitation of LTE, that introduced by Rupprecht *et al*. [21] and then considered in [31] was deployed by using a customized version of openLTE installed on a USRP B210 [23]. By exploiting the reject causes messages that are transmitted without any integrity protection, an attacker will create a rogue eNodeB that will reject the UE from accessing LTE services. Thus according LTE standards, to accept certain reject cause messages, the UE and network may not perform any mutual authentication and security context [32]. When the E-UTRAN is being used by UE, the EPS mobility management (EMM) protocol provides mobility control procedures. The EMM protocol also brings the NAS protocols security control [33].

In this section we define two of EMM case massage that are sent from a rogue eNodeB for reject the UE from accessing LTE services. Even before transmission of “TAU Reject” messages requires no security keys, the rogue eNodeB could target any LTE mobile user in its area for provisional Dos. A similar threat is also possible for “Service Reject/Attach Reject” messages. Whenever the UE transmits a ‘TAU Request’ message to a rogue eNodeB, it would still be associated to the real network; this message is also integrity protected but not encrypted under the NAS security context. This will be an opportunity for the attacker who could easily decode it and respond with a “TAU Reject” message (EMM cause number 8 EPS services and non-EPS services not permitted) that does not require integrity enforcement as per LTE requirements. Figure 4, the UE will accept the reject cause and continue to act further by deleting all existing services connected to the actual network. In addition, TAU Attach requests will not be searched for or sent by the UE to any nearby legitimate LTE network, causing temporary DoS and with less effect [32].

This similar attack can also be taken over by responding to any mobile device with a reject message. Put it differently, the base station is not yet authenticated when the attach reject message is sent, but the UE has to follow the attach reject message. If a rogue base station responds with an attach reject message to an incoming signal, it may trick the mobile device into assuming it is not authorized to connect to that given network. Accordingly, the system would avoid requesting to connect to any of the provider’s base stations that the rogue eNodeB was spoofing. Figure 5, demonstrates this exploit in which a rogue base station effectively prevents any mobile device from connecting to the network in its radio communication range, resulting in a DoS [18].

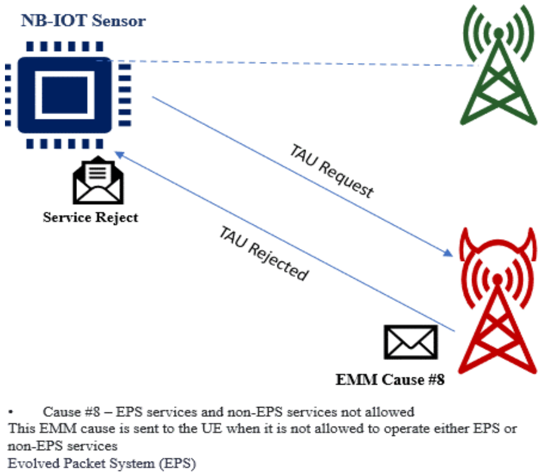

NB-IOT Sensor
Service Reject
TAU Request
TAU Rejected
EMM Cause #8
• Cause #8 – EPS services and non-EPS services not allowed
This EMM cause is sent to the UE when it is not allowed to operate either EPS or non-EPS services
Evolved Packet System (EPS)

Figure 4. Deny both LTE and non-LTE services

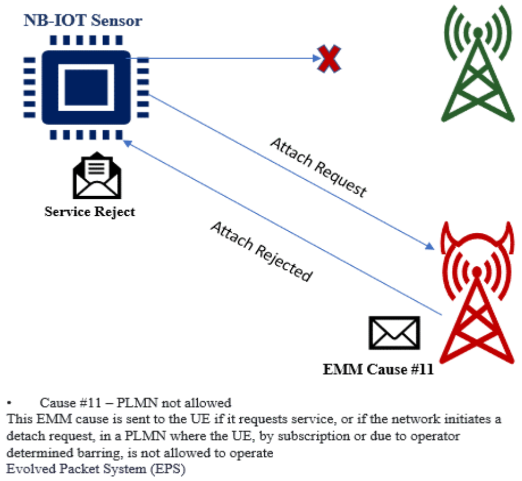

NB-IOT Sensor
Service Reject
Attach Request
Attach Rejected
EMM Cause #11
• Cause #11 – PLMN not allowed
This EMM cause is sent to the UE if it requests service, or if the network initiates a detach request, in a PLMN where the UE, by subscription or due to operator determined barring, is not allowed to operate
Evolved Packet System (EPS)

Figure 5. Mobile device temporary block by a rogue LTE base station

5. CONCLUSION

This paper presented an overview of the current threat and vulnerabilities in the cellular telecommunications radio subnet, which is the communication platform of NB-IoT sensors. Eavesdropping is one of the main privacy issues which is considered in the presented article. the hackers could actually use a connected device to IoT networks to virtually invade a person’s privacy. Regard to the connection of NB-IoT sensors to eNodeBs in the fourth-generation network and the existence of various vulnerabilities in E-UTRAN, this research has investigated and implemented attack scenarios in the radio network against NB-IoT sensors. The vulnerabilities that have been considered in this study are divided into two main categories: sniffing and communication disorders. We described two attack scenarios that open source and SDR tools have been used to emulate these attacks. The first step is to implement rogue eNodeB as an IMSI catcher. With this invasive element in the radio network, IMSI of sensors connected to the network can be found.

Although these IMSI values are rarely exchanged on the network, their values can be sniffed and extracted by exploiting a vulnerability in the radio network that forced sensors to disconnect from the network and resend a connection request. In this condition, another vulnerability in the LTE radio network with rogue eNodeB can be used to execute the denial-of-service attack. To execute this scenario, the attacker uses a fake station, in response to "Attach Request" and "TAU Request" sent by the sensors, sends "Reject" messages. Therefore, the sensors cannot be connected to the real station and will lose their efficiency if not connected to the legitimate LTE network.

REFERENCES

[1] J. Granjal, E. Monteiro and J. Sá Silva, "Security for the Internet of Things: A Survey of Existing Protocols and Open Research Issues," in *IEEE Communications Surveys & Tutorials*, vol. 17, no. 3, pp. 1294-1312, 2015, doi: 10.1109/COMST.2015.2388550.

[2] S. R. Taghanaki, S. B. Arzandeh and A. Bohlooli, "A Decentralized Method for Detecting Clone ID Attacks on the Internet of Things," *2021 5th International Conference on Internet of Things and Applications (IoT)*, 2021, pp. 1-6, doi: 10.1109/IoT52625.2021.9469723.

[3] Future Generation Computer Systems, vol. 29, no. 7, pp. 1645-1660, Sep. 2013.

[4] N. Meghanathan, S. Boumerdassi, N. Chaki, and D. Nagamalai ''Recent Trends in Network Security and Applications," *Third International Conference, CNSA 2010, Chennai, India, July 23-25, 2010 Proceedings*, vol. 89, 2010, doi: 10.1007/978-3-642-14478-3.

[5] R. Ratasuk, B. Vejlgaard, N. Mangalvedhe, and A. Ghosh, "NB-IoT system for M2M communication," *2016 IEEE Wireless Communications and Networking Conference*, Doha, Qatar, 2016, pp. 1-5, doi: 10.1109/WCNC.2016.7564708.

[6] L. Alliance, "LoRaWAN specification. LoRa Alliance," *Tech. Rep*. 2015.

[7] S. Sigfox, "One Network a Billion Dreams," *M2M and IoT Redefined Through Cost Effective and Energy Optimized Connectivity. (White Paper)*, 2016.

[8] J. Sanchez-Gomez, D. Garcia-Carrillo, R. Marin-Perez, and A. F. Skarmeta, "Secure Authentication and Credential Establishment in Narrowband IoT and 5G," *Sensors*, vol. 20, p. 882, 2020, doi: 10.3390/s20030882.

[9] N. Yousefnezhad, A. Malhi, and K. Främling, "Security in product lifecycle of IoT devices: A survey," *Journal of Network and Computer Applications*, vol. 171, Dec. 2020, doi: 10.1016/j.jnca.2020.102779.

[10] K. S. Mohamed, "IoT Networking and Communication Layer," *In: The Era of Internet of Things. Springer, Cham*, 2019, doi: 10.1007/978-3-030-18133-8_3.

[11] M. S. Mahmoud and A. A. Mohamad, "A study of efficient power consumption wireless communication techniques/modules for internet of things (IoT) applications," 2016, doi: 10.4236/ait.2016.62002.

[12] V. Kumar, R. K. Jha, and S. Jain, "NB-IoT Security: A Survey," *Wireless Pers Commun.*, vol. 113, pp. 2661–2708, 2020, doi: 10.1007/s11277-020-07346-7.

[13] K. Meta, "Implementation of an Embedded RTOS FW platform for data transceivers on 2G/3G/4G/5G mobile network," *Diss. Politecnico di Torino*, 2023.

[14] S. Lucero, "IoT platforms: enabling the Internet of Things," *White paper*, 2016.

[15] S. Forge and K. Vu, "Forming a 5G strategy for developing countries: A note for policy makers," *Telecommunications Policy*, vol. 44, no. 7, p. 101975, Aug. 2020, doi: 10.1016/j.telpol.2020.101975.

[16] M. Chen, Y. Miao, Y. Hao and K. Hwang, "Narrow Band Internet of Things," in *IEEE Access*, vol. 5, pp. 20557-20577, 2017, doi: 10.1109/ACCESS.2017.2751586.

[17] J. Afzal, "NB-IoT-Data Rates and Latency," *SIGFOX*. [Online]. Available: https://www.netmanias.com/en/?m=view&id=blog&no=12609. (accessed, 16 Aug. 2017).

[18] R. P. Jover, "LTE security, protocol exploits and location tracking experimentation with low-cost software radio," *arXiv preprint arXiv:1607.05171*, 2016.

[19] D. Rupprecht, K. Kohls, T. Holz, and C. Poepper, "IMP4GT: Impersonation attacks in 4G networks," *Proceedings 2020 Network and Distributed System Security Symposium*, 2020, doi:10.14722/ndss.2020.24283.

[20] C. M. Ernesto, P. M. L. Fernando, P. P. I. Patricia, and C. P. G. Alonso, "Mission Critical Communication System with Cognitive Radio Networks using SDR," *2020 IEEE XXVII International Conference on Electronics, Electrical Engineering and Computing (INTERCON)*, Lima, Peru, 2020, pp. 1-4, doi: 10.1109/INTERCON50315.2020.9220235.

[21] D. Rupprecht, A. Dabrowski, T. Holz, E. Weippl, and C. Pöpper, "On Security Research Towards Future Mobile Network Generations," in *IEEE Communications Surveys & Tutorials*, vol. 20, no. 3, pp. 2518-2542, 2018, doi: 10.1109/COMST.2018.2820728.

[22] A. Shaik, R. Borgaonkar, N. Asokan, V. Niemi, and J.-P. Seifert, "LTE and IMSI catcher myths," 2015.

[23] N. Nikaein, M. K. Marina, S. Manickam, A. Dawson, R. Knopp, and C. Bonnet," OpenAirInterface: A flexible platform for 5G research," *ACM SIGCOMM Computer Communication Review*, vol. 44, no. 5, pp. 33-38, 2014, doi: 10.1145/2677046.2677053.

[24] L. Chaparro and A. Akan, "Chapter 8—Sampling Theory," in *Signals and Systems Using MATLAB (Second Edition)*, 2015, pp. 493-534.

[25] I. Palamà, F. Gringoli, G. Bianchi, and N. Blefari-Melazzi, "IMSI catchers in the wild: A real world 4G/5G assessment," *Computer Networks*, vol. 194, p. 108137, Jul. 2021, doi: 10.1016/j.comnet.2021.108137.

[26] C. Yu, S. Chen, F. Wang, and Z. Wei, "Improving 4G/5G air interface security: A survey of existing attacks on different LTE layers," *Computer Networks*, vol. 201, p. 108532, Dec. 2021, doi: 10.1016/j.comnet.2021.108532.

[27] R. P. Jover, J. Lackey, and A. Raghavan, "Enhancing the security of LTE networks against jamming attacks," *EURASIP J. on Info. Security*, vol. 7, pp. 1-14, 2024, doi: 10.1186/1687-417X-2014-7.

[28] M. Lichtman, R. Rao, V. Marojevic, J. Reed and R. P. Jover, "5G NR Jamming, Spoofing, and Sniffing: Threat Assessment and Mitigation," *2018 IEEE International Conference on Communications Workshops (ICC Workshops)*, Kansas City, MO, 2018, pp. 1-6, doi: 10.1109/ICCW.2018.8403769.

[29] Q. Yang and L. Huang, "Mobile Network Security," Inside Radio: An Attack and Defense Guide, pp. 267–342, 2018, doi:10.1007/978-981-10-8447-8_8.

[30] S. Sesia, M. Baker, and I. Toufik, "LTE, The UMTS Long Term Evolution: From Theory to Practice," *John Wiley & Sons*, 2009, doi: 10.1002/9780470978504.

[31] R. P. Jover, “LTE security and protocol exploits,” *2016 ShmooCon Proceedings*, Jan. 2016.
[32] K. Vachhani, “Security Threats Against LTE Networks: A Survey,” *6th International Symposium, SSCC 2018*, Bangalore, India, Jan. 2019, pp. 242-256, doi: 10.1007/978-981-13-5826-5_18.
[33] C. Yu and S. Chen, “On Effects of Mobility Management Signalling Based DoS Attacks Against LTE Terminals,” *2019 IEEE 38th International Performance Computing and Communications Conference (IPCCC)*, London, UK, 2019, pp. 1-8, doi: 10.1109/IPCCC47392.2019.8958725.

BIOGRAPHIES OF AUTHORS

Ali Abdollahi received his degree in Information Technology Engineering. He is an invited speaker and trainer to many international conferences. His main research interests are network communications and application security. He can be contacted at email: ali.abdollahi19@gmail.com.

Shohreh Behnam Arzandeh received the M.S. degree in Information Technology from Islamic Azad University, Olumtahghighat Branch in 2020. Her main research interests are internet of things, computer network security, and routing protocols. She can be contacted at email: Shohreh.b.arzandeh@gmail.com.

Mohsen Sheibani received the M.S. degree in Computer Science from Islamic Azad University, Najafabad Branch, Isfahan, Iran, in 2019. His main research interests are network security, IoT, wireless systems, and machine learning. He can be contacted at email: sheibani.mohsen01@gmail.com.