Security threats of NB-IoT and countermeasures

Adam U Mentsiev¹,³ and Tamirlan R Magomaev²

¹ Faculty of information technology, Chechen State University, 32 Sheripov Street, Grozny, 364024, Russia
² Department of Information Systems in Economic, Institute of Digital Economics and Technological Entrepreneurship, GTSU named after Acad. M.D. Millionschikov, 100 Isaev Avenue, Grozny, 364061, Russia
³ E-mail: a.mentsiev@chesu.ru

Abstract. IoT technology is already an integral part of our business and social life. This technology can be seen in almost every big city in Russia. Many leading countries are at a relatively high level of mass adoption of the Internet of Things technology. Many areas of the country's activity are directly dependent on the Internet of things: “smart house”, “smart city”, digital agriculture, automation of production, Industry 4.0, etc. At the same time, it is necessary to take into account the fact that the multifaceted use of technology entails a special interest of attackers and an increase in security threats. Here, for specialists, the question of ensuring security arises. This article discusses the characteristics of the Internet of things devices, the main threats to the security of the narrowband Internet of things and provides recommendations for countermeasures.

1. Introduction

Internet of Things (IoT) is one of the biggest and fastest-growing inventions of the last decade and the growth in this industry can be estimated by the sheer number of devices connected to the Internet of Things Network. In developed countries, IoT connected devices have very much become a part of daily life. The number of these devices connected to the IoT network has crossed over 26.66 billion by the end of 2019 and it is only growing as there are 127 new devices being connected to the web every second around the world [1]. What does this ever-increasing number of devices mean you may ask? The more the number of devices connected to the IoT network the more vulnerable it becomes to a variety of threats and security risks. Many IoT devices that are hooked to the internet handle data of extremely sensitive nature which should only be accessed by authorized personnel. These applications are computer programs that are most of the time using real-time conditions to ensure successful completion of tasks.

One of the reasons behind this vulnerability to security risks is that the manufacturers of the devices that are being connected to the IoT networks do not take the privacy or security of the device and data as a priority. Hence many users unaware of this still buy these devices and connect them to the IoT network increasing the risk of security breaches etc. [2]

2. Characteristics of IoT devices

We are going to discuss some of the characteristics of IoT devices that make them vulnerable to security threats. This is in order to identify the characteristics that lead to a problem in order to find a solution to
that problem. If we look at the basic definition of the Internet of Things, we’ll find what is the root cause of all these security threats. Internet of Things is a collection of billions of devices all around the world which is connected to each other via the internet [3]. Not only that these IoT devices are also connected to the cloud via the World Wide Web in order to share data with other IoT devices and thus become vulnerable to hackers all around the world. Some main characteristics of IoT devices include:

- They collect real time data in order to perform their tasks,
- They are constantly making the use of cellular LPWAN which is also called Narrowband IoT and LTE-M,
- These devices are measuring physical parameters and are capable of carrying out physical actions,
- They are permanently connected to the cloud, and lastly
- These devices have the ability to make a decision all by themselves based on the data present [4].

3. Security threats of narrowband IoT

The above-discussed characteristics give us a peek into the nature of challenges faced by narrowband IoT. We are now going to discuss these many challenges and the reason why many IoT devices face these challenges. One of the biggest misunderstandings that are in the market related to IoT security is that it only means making the IoT devices more secure, whereas it is much more than that [5]. When we say IoT we mean a complete system and not just everyday use devices, this system includes the device itself, cloud, the mobile application which is being used to control the device, the network interface that the device is connected to, the software being run on the system, use of encryption, authentication and finally the physical security of both the device and every other physical component [6]. So along with the IoT device, all these components of the system are equally vulnerable to the security threats and challenges that we are going to discuss. Let us now dive into these challenges one by one.

3.1. Poor application and end-point security

As the English phrase goes, “A chain is as strong as its weakest link”. The case with IoT systems is very much similar. No matter how good the security overall is, if you are using a device that has poor security, the whole system can be easily compromised [7]. This goes for application security as well. These poorly secured applications and end-point devices make the systems vulnerable to cyber-attacks. One of the biggest reason behind this is that most device manufacturers are the same who used to manufacture devices before the advent of IoT, while they have now made their devices smart in order to be connected to IoT but they have not focused on the security viewpoint because it is not an essential feature for them. Similar is the case with the application developers, all these people are not mature from a security standpoint and they treat these applications like all other random applications for mobile phones, etc. However, security is a crucial feature of an IoT device or an application and needs to be considered as much as the quality or functioning of the product [8].

3.2. Insufficient authorization/authentication

As discussed before all IoT devices require some form of authorization or authentication in order to make them secure from data theft or other security risks. But even to this day, most devices being produced in the commercial market come with processors so small that they are only designed to perform very basic tasks only and cannot process something like authorization or authentication which requires a larger processor. You may think how much processing power does a simple task as authentication may require but you’d be wrong to assume that most commercial devices even possess the power to do that [9].

3.3. Lack of physical security

The whole idea behind the Internet of Things is to create modern and smart cities in which each and every device of each and every house interacts and shares data with the system in order to smartly run
the system. This means that most IoT devices are in urban settings and are exposed to the public [10]. Moreover, urban infrastructure can sometimes be very complicated and dense to an extent where it is impossible to provide physical security for the system. This increases the risk of a physical attack and by physical attack, we do not mean that some criminal would damage the system, but it could mean that the hackers can easily access the IoT system that is out in the public and can tap into the system in order to steal data and make devices mal-operate [11].

3.4. Excessive amount of sensitive data
A smart device is the one that has some basic built-in functions as a microphone, camera or night vision, etc. which it requires to receive, transmit data and interact with the user. These functions are acting like the eyes and ears of the device and are continuously recording terabytes of data sometimes without the knowledge of the user using these devices [12]. This data can be very sensitive and if fallen into wrong hands it can violate the privacy of the user and can become a serious security threat. This is one of the biggest reasons that people are unable to trust IoT systems with security and privacy issues and there have been hundreds of reported cases where the collectors of data have misused the data and violated many data privacy laws [13].

3.5. Insecure default credentials
When you purchase a new IoT device or any device for that matter, it usually comes with a default username and a default password that you use in order to log in for the first time into the device. This default username and password are called default credentials and can be a huge security risk. Some of the IoT devices even to this day come with hard-coded passwords and usernames which means that these credentials can never be changed and are sometimes imprinted on the device. This makes the device vulnerable to not only cyberattacks but also physical attacks where someone might get access to the default username or password. Even if it is not hard-coded some users might not bother changing these credentials thus making their devices more insecure. In such cases, hackers always try to access the devices using a default username and password and can easily get in [14].

4. Countermeasures
There are a number of countermeasures that can be taken in order to ensure the security of the IoT systems. These countermeasures include the involvement of everyone from the user, to manufacturers and application developers, etc. Here are some of the steps that each one of us needs to ensure before they can switch to smart devices that are connected to IoT.

First and the most important step that the manufacturers and application developers need to take is to realize the importance of security in the IoT devices and start treating it as a priority rather than a feature. All the new IoT devices being manufactured and all the IoT applications that are being developed should be secure from end to end and should not allow the leak of data from their end. As a user what we can do to ensure secure applications and end-point is while purchasing these devices or installing an application we need to make sure it is from a reliable manufacturer or developer. Most of the brands in the market are reliable from a security standpoint, the problem only arises when manufacturers from local markets try to push their product in the market without a focus on the security [15].

The second most crucial step that needs to be taken is the need for authentication and authorization on the use of smart devices that are being connected to IoT. Manufacturers and developers need to make sure that their devices and applications support secure authorization and authentication. Users also need to ensure that the device they are purchasing has this as a built-in feature. For devices that are already in operation but do not support even basic features like authentication and authorization, aftermarket applications and devices can be used which provide extra security in the form of authentication or authorization. The user also needs to ensure that they do not purchase devices with hard-coded default credentials and as soon as they get a device they change the credentials.
From a data standpoint, user data is one of the major components that add to the risk and needs to be handed in a secure manner. Data collectors and vendors need to make data security their top priority and need to ensure the safe transaction of data from one device to another. Governments all around the world have a huge role to play in this step and they need to make sure that the data providers, application developers, etc. are not misusing the user data from general public. Special laws and regulations need to be put forward in order to stop these people from misusing the public data [16].

Another important step that needs to be taken is the presence of a monitoring system, which is monitoring the whole system from device end-point to network security etc. and in the case of an accident, it is always there to detect the weakest link the chain and take a responsive action in order to stop the accident from happening again. The application being used in IoT systems should come with built-in functionalities to record abnormalities in the data and later report it so that the user can take action accordingly.

Last but not least, a multiple layer system needs to be put in place in order to protect the IoT system which itself is a complex interconnected system. These multiple layers must include administrative, technical and physical controls that are always in place to protect the IoT network in the face of any adversity and are always there to take action. Without a sufficient amount of security and protection of data, IoT cannot and will not remain successful in the long run and is bound to fail. So it is upon the management, manufacturers, developers and the users themselves to make security the number one priority when dealing with devices connected to IoT.

References
[1] Malik H, Alam M M, Pervaiz H, Moullec Y L, Al-Dulaimi A, Parand S and Reggiani L 2019 Radio Resource Management in NB-IoT Systems: Empowered by Interference Prediction and Flexible Duplexing. *IEEE Network* 34 144-51
[2] Cavo L, Fuhrmann S and Liu L 2020 Design of an area efficient crypto processor for 3GPP-LTE NB-IoT devices. *Microprocess. Microsystems* 72 1-24
[3] Cao J, Yu P, Xiang X, Ma M and Li H 2019 Anti-Quantum Fast Authentication and Data Transmission Scheme for Massive Devices in 5G NB-IoT System *IEEE Internet of Things Journal* 6 9794-805
[4] Huang H and Zhang L 2019 Reliable and Secure Constellation Shifting Aided Differential Radio Frequency Watermark Design for NB-IoT Systems *IEEE Communications Letters* 23 2262-65
[5] Jeon W S, Seo S B and Jeong D G 2018 Effective Frequency Hopping Pattern for ToA Estimation in NB-IoT Random Access *IEEE Transactions on Vehicular Technology* 67 10150-54
[6] Karaagac A, Dalipi E, Crombez P, Poorter E D and Hoebeke J 2019 Light-weight streaming protocol for the Internet of Multimedia Things: Voice streaming over NB-IoT *Pervasive and Mobile Computing* 59 1-22
[7] Li W, Zhang Q, Zhang Q, Guo F, Qiao Sh, Liu Sh, Luo Yu, Niu Yu and Heng X 2019 Development of a distributed hybrid seismic-electrical data acquisition system based on NB-IoT technology *Geoscientific Instrumentation, Methods and Data Systems Discussions* 8(2) 177-86
[8] Andres-Maldonado P, Ameigeiras P, Prados-Garzon J, Navarro-Ortiz J and Lópex-Soler J M 2019 An Analytical Performance Evaluation Framework for NB-IoT *IEEE Internet of Things Journal* 6(4) 7232-40
[9] Martiradonna S, Piro G and Boggia G 2019 On the Evaluation of the NB-IoT Random Access Procedure in Monitoring Infrastructures *Sensors* 19(14)
[10] Nguyen N H, Berscheid B and Nguyen H H 2019 Fast-OFDM with Index Modulation for NB-IoT *IEEE Communications Letters* 23(7) 1157-60
[11] Liu DZ, Guo ST, Yang YY, Shi YW and Chen MG 2019 Geomagnetism-Based Indoor Navigation by Offloading Strategy in NB-IoT *IEEE Internet of Things Journal* 6(3) 4074-84
[12] Andres-Maldonado P, Lauridsen M, Ameigeiras P and Lopez-Soler JM 2019 Analytical Modeling and Experimental Validation of NB-IoT Device Energy Consumption IEEE Internet of Things Journal 6(3) 5691-701

[13] Jiang N, Deng YS, Nallanathan A and Chambers JA 2019 Reinforcement Learning for Real-Time Optimization in NB-IoT Networks IEEE Journal on Selected Areas in Communications 37(6) 1424-40

[14] Cao J, Yu P, Ma MD and Gao WF 2019 Fast Authentication and Data Transfer Scheme for Massive NB-IoT Devices in 3GPP 5G Network IEEE Internet of Things Journal 6(2) 1561-75

[15] Liu PC, Guo B, Zhang Y, Han YH, Liu Y and Wang GZ 2019 NB-IoT Network and Service Collaborative Optimization Signal and Information Processing, Networking and Computers (ICSINC) 550 505-15

[16] Zhang N and Liu Y 2019 NB-IOT Drives Intelligent Cold Chain for Best Application Proceedings of 2019 IEEE 9th International Conference On Electronics Information and Emergency Communication (ICEIEC 2019) 188-91