Wireless Personal Communications (2020) 113:2661–2708
https://doi.org/10.1007/s11277-020-07346-7

NB-IoT Security: A Survey

Vinod Kumar[1] · Rakesh Kumar Jha[2] · Sanjeev Jain[3]

Published online: 15 April 2020

Abstract
In the past few years, the term Internet of Things (IoT) has become very prevalent. In IoT, aggregation of data (from sensors) to processing the data (to the cloud) is energy constraint. To address this challenge, Narrowband- Internet of Things (NB-IoT) is becoming a popular choice for smart devices manufacturer due to its characteristics of high energy-efficient and long battery life. Researchers and academia have addressed the problem related to energy constraints, but it opens the door for security issues related to NB-IoT devices. In this paper, we have done a survey closely related to security issues related to NB-IoT technologies like RFID, WSN, WoT, and IoT. IoT is enabled with five-layered architectures, and each layer is *prone* to different security attacks. In this paper, we have provided a comparative analysis of security issues in a layer-based approach. We propose the different possible security attacks like shared node attack, synchronization attack, node failure attack, source code attack, and battery drainage attack associated with NB-IoT. To do the performance analysis of security attacks, related matrix, and their mathematical formulation is based on Secrecy Rate and Secrecy Outage Probability for the smart home application. This paper also raises security issues related to smart health and smart agriculture applications.

Keywords Internet of Things (IoT) · Narrowband-Internet of Things (NB-IoT) · Resource allocation · Security issues · Secrecy rate (SR) · Secrecy outage probability (SOP)

✉ Rakesh Kumar Jha
jharakesh.45@gmail.com

Vinod Kumar
vkgupta1982@gmail.com

Sanjeev Jain
dr_sanjeevjain@yahoo.com

[1] School of Computer Science Engineering, Shri Mata Vaishno Devi University, Katra, J&K, India

[2] School of Electronics and Communication Engineering, Shri Mata Vaishno Devi University, Katra, J&K, India

[3] IIITDM Jabalpur, Jabalpur, Madhya Pradesh, India

1 Introduction

For the last few years, the way of using technical devices, home appliances, instruments, and other objects have changed according to the reliability of the users. Due to which, IoT concept is increasing exponentially to make human life more relaxed and comfortable, which has led to a rise in data transfer and storage related to security is also increasing rapidly. IoT gives an image of the future Internet where every computing device, things of daily life, and every user has sensing and actuating capabilities. All of these cooperate and communicate with each other according to their convenience and economic benefit [1]. IoT is associated with the various concepts coming from Radio Frequency and Identification (RFID), Wireless Sensor Network (WSN), Web of Things (WoT) and Smart Things.

If IoT is combined with the cloud, it provides the benefit of integrating the Cyber-Physical System (CPS) with Supervisory Control and Data Acquisition (SCADA) [2]. Many essentials functional and nonfunctional requirements of IoT middleware technologies are defined, such as resource recovery, resource management, data, code and event management, scalability, reliability, availability, and security. The author in [3] explains the role of service-oriented middleware architecture design in IoT based on Service-oriented Computing.

Third Generation Partnership Projects (3GPP), in their radio access network plenary meeting, have decided to standardize the NB-IoT, which gives better indoor coverage, supports a large number of low-throughput devices, and better utilization of resource block [4]. Social IoT (SIoT) describes a world where the objects around human beings can intelligently sense and are motivated by various social networks over huge Internet sites such as Facebook, WhatsApp, Twitter, and Instagram [5]. The three-layer system model defined in [6] gives the concept of social IoT, based on the "trust management and security in the IoT world" by defining the exploitability matrix and impact matrix. The authors in [7] proposed an encapsulation of RFID messages for IPv6 packet for each IoT node so that each element or node is within reach of another node in the network. It also defines web squared, which is the evolution of Web 2.0.

Different IoT research areas and their challenges have been explained by authors in [8], which are related to security and standardization. IoT supports establishing connections and designing networks between two different objects in various heterogeneous environments. Confidentiality, integrity, availability, less space, and power consumption are the necessities of any IoT algorithm. Authors have proposed a Hybrid lightweight algorithm (HLA) [9] by combining the two lightweight asymmetric and asymmetric encryption algorithms. By using the Near-Threshold Computing (NTC) method, it reduces the power consumption, as compared to the standard voltage. The author in [10] aims to study the security of post-quantum cryptography and implement a cryptosystem based on these problems. This mathematical problem evaluates the performance in a real-time deployed network—the research project named Crypto-MathCREST supported by a Japanese agency named Japan science and technology. A lightweight protocol for IoT application is a transfer protocol, designed at the Internet Engineering Task Force (IETF), named [11] Constrained Application Protocol (CoAP). The author in [12] proposed a model for IoT, having a limited budget for protecting the device communication where computation time is very less, but the key size is large. In another case, he combined FPGA with Moore's law and calculated the cost of breaking the security of the cryptosystem having a small key size. He showed that the cost of a cryptosystem decreases rapidly if the key size is small and suitable for IoT devices.

Various attacks on smart wearable devices (such as man-in-the-middle, mole attack, and mule attack) and its countermeasures are described in brief [13]. A lightweight game theoretic technique based on the Nash equilibrium concept [14] is used to activate an anomaly detection technique when a new attack's signature is expected to occur. The relation between the time spent on analyzing the traffic volume and the time instance to patch the AP's are analyzed in [15]. It proposed the patching of intermediate nodes, for preventing the redirection of malicious traffic, and introduced the DDoS attack, launched by the IoT botnets. The main requirement of IoT applications is to develop such protocols that are compatible with low power IoT devices. These protocols scale up to enormous storage of data in the cloud. As the low power IoT devices may work for 10–20 years, so it is required to secure today's devices against the attacks for the next 20 years [16].

In LPWAN technologies, on both licensed and unlicensed spectrum, the unlicensed spectrum consists of Long Range (LoRa) and SIGFOX, while the licensed spectrum consists of LTE-M and NB-IoT technology. All these technologies use a narrowband spectrum and suitable for small data, sent over a large area, by the object and maintains the battery life over the years. In [17], author(s) introduced a method of non-orthogonal multiple access (NOMA) to overcome the limitation of system capacity and also defined LTE-M and LTE-N techniques for machine type communication and Narrowband IoT Category. Power consumption analysis, effective bandwidth, and transmission time analysis for LPWAN are performed in [18, 19]. 3GPP standardized two LTE operated technologies called eMTC (enhanced Machine Type Communication) and NB-IoT in release-13. eMTC works with relatively large data transmission ($\leq$1 Mb/s) as compared with NB-IoT (160–250 kbps(DL), 160–200 kbps(UL), low mobility and high coverage (~17 km in suburban and ~5 km in urban) while NB-IoT is designed to achieve better performance as compared to eMTC [16].

1.1 Contributions and Organization

This paper provides a detailed analysis of possible security attacks on NB-IoT enabled devices, with proposed approaches and techniques related to smart home and smart health care applications.

Our contributions in the paper are summarized below:

- This paper cogitates the security perspectives of RFID, WSN, and WoT used in the evolution of IoT and NB-IoT through proposed architecture.
- Analyze the possible security attacks on different layers of IoT and NB-IoT.
- Provide a detailed analysis of different possible attacks on NB-IoT.
- Proposed possible attacks on NB-IoT with proposed architecture and detail mathematical analysis such as Node failure attack, shared node attack, and synchronization attack.

The layout of this paper is shown in Fig. 1. This section of the paper provides the background of the basic concept of IoT and associated security issues with IoT and NB-IoT. Section 2 gives an introduction of technologies like RFID, WSN, WoT with security provision, used in IoT advancement. Section 3 contains definitions of various security matrices, a table of detailed layer-wise security attacks, techniques, or methods proposed by various authors for IoT scenarios and various challenges related to IoT. Section 4 provides a brief idea about NB-IoT operation modes. The network architecture has been proposed in this section. Section 5 is the most significant section, describe different possible attacks on

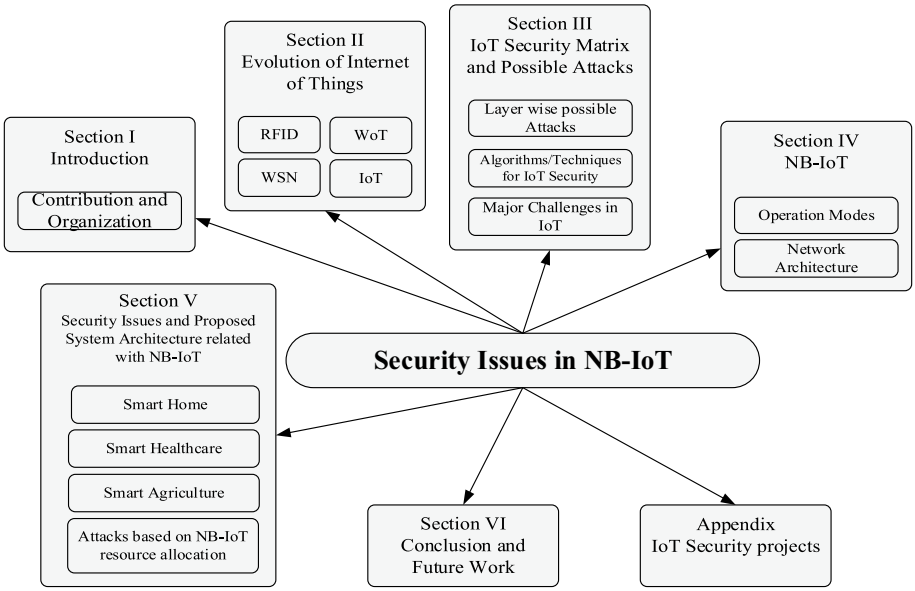


Fig. 1 Organization of the survey on NB-IoT

NB-IoT devices based on applications such as smart home, critical smart healthcare. In this section, we have also proposed a system model and security issues for NB-IoT and have given the mathematical formulation and methods for solving these attacking scenarios. Resource allocation based possible attacks and proposed attacks are defined in this part of the paper. Section 6 concludes this paper with future work. Additionally, the appendix provides the list of research projects working on IoT security and the list of abbreviations.

2 Evolution of Internet of Things

The number of intelligent wireless devices is increasing in an exponential way, in which data availability, data transfer speed, power requirement, and security issue is playing a pivotal role. In wireless automation, if we go back before the era of the Internet, fixed, mobile telephony, and short messaging services (SMS's) came into existence. After advancement in the Internet, there has been an age of emails, e-commerce, social media, and smart things. Different sensing technologies like RFID, WSN, and other technologies like machine-to-machine communication (M2M), SCADA has been introduced in the development of the IoT. In recent years, IoT has become a part of the global Internet and consists of billions of intelligent devices communicating with each other by using the Internet. Its growth is going on the way of IoT to the Internet of Everything (IoE).

Figure 2 shows the development of IoT and further NB-IoT technology, in terms of the number of users, technology growth, and frequency spectrum used. It provides the details of year wise technology evolution from RFID to NB-IoT with their applications. Table 1 provides the assessment among RFID, WSN, and WoT.

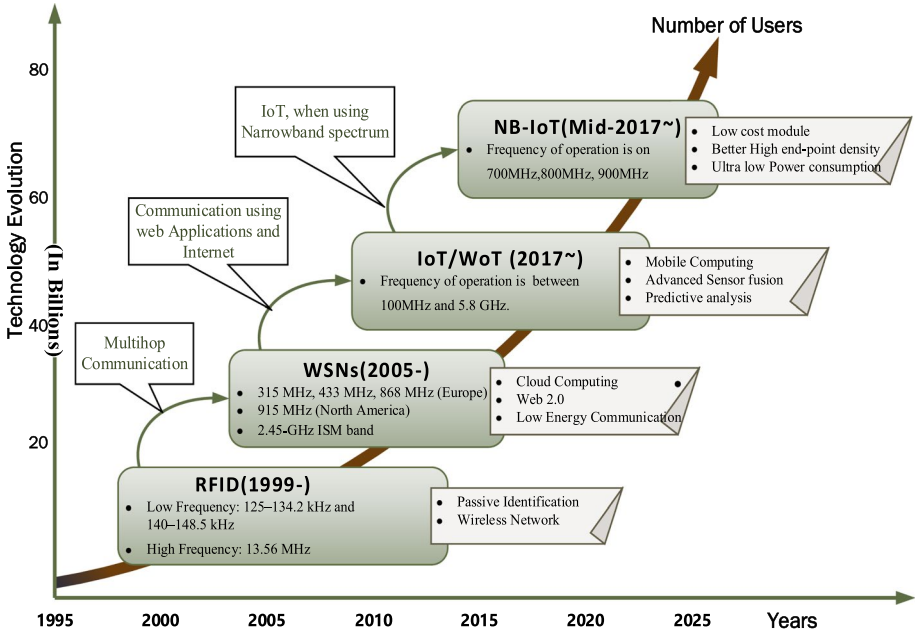


Fig. 2 Evolution of RFID → IoT/NB-IoT *Source*: Statista (2018)

2.1 Radio Frequency Identification (RFID)

In the evolution, IoT technology identification and tracking enabled technology, which came into existence in the 80 s, about 3 decades ago, are being used worldwide in the form of RFID tag. The first patent filed by Mario W. Cardullo, on active RFID tag consists of rewritable storage, in 1973 in the United States. Subsequently, the evolution of IoT technology in 1999, RFID has taken the backside of connected sensors. In 2004, Juels [20] had been proposed yoking protocol, for providing cryptographic proof to scan two RFID tags simultaneously.

International Standards Organization (ISO) and Electronics Product Code Global (EPC Global) are the two central standardization bodies, incorporated into standardizing the RFID technology [21]. This radio sensing technology utilizes radio waves for automatic identification of objects from the RFID tag of smart labels. These tags may be passive or powered by battery as per the requirements of the objects.

Figure 3 shows the system architecture for the RFID tag cloning attack (A1–A4), and its detection by using the BASE algorithm [22]. A passive cloning attacker launches the cloning attack and injects the clone tags. These cloned tags work the same as the genuine tags and are hard to distinguish. It gives a proper response to the RFID reader queries so that detection protocol fails to detect the cloned tag. The workflow of this baseline protocol (P1–P4) is shown in Fig. 3. A detection approach is fed on ID cardinality, as input in the BASE algorithm. If the tag cardinality is higher than the ID cardinality (ALOHA frame size), the clone is detected. Otherwise, it's not detected. This approach is mainly coordinated by an RFID reader, which queries from clone tags (step-P2), and the reply comes from the tag (step-P3). Based on the response from the reader, the clone

Table 1 Comparison of RFID/WSN/WoT in IoT evolution

Technology	RFID	WSN	Web/Internet of Things
Mobility support	Tags move with attached objects	Usually static	Both static as well as dynamic
Database requirement	Yes	Yes	Yes/greatly
Range of frequency	High freq: 13.56 MHz Low freq: 125–134.2 kHz and 140–148.5 kHz	315, 433, and 868 MHz (Europe) 915 MHz (N.A.), 2.45 GHz ISM band	The frequency of operation is between 100 MHz and 5.8 GHz
Power requirement	Battery-powered or passive	Battery-powered	Battery powered
Security provision	Less	Less	Moderate
Encryption algorithm used	DES, AES, SecureRF, DESL	DES, 3DES, DES-X, blowfish, TEA, XTEA, AES, HEIGHT	ECC, Diffie-Hellman, COSE
Possible security techniques	Optimistic trivial RFID authentication protocol (O-TRAP)	Route optimization algorithm, active Trust, Q-s composite, TinySec, SPINS, LSec, LISA, and LISP	REST, HTTP, JWT, CWT, Web Sockets, TLS, DTLS

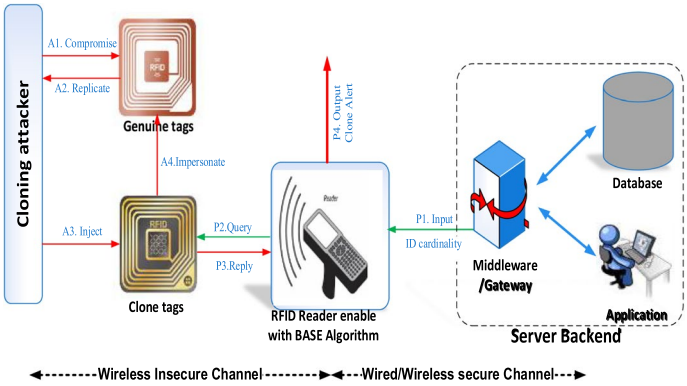


Fig. 3 RFID system model with cloning attack and detection [22]

sends alert as an output (step-P4). In the next iteration, the system proposed in Fig. 3 is detached from clone tags (clone free) operations.

As per RFID security concern, tag counterfeiting and tag encoding are the essential aspects of maintaining the integrity of tag. In a situation when multiple RFID tags transmit data to the RFID reader simultaneously, conflict in data may occur. This problem can be solved by applying anti-collision techniques. Multiple security threats, such as reverse engineering attack, power analysis attack, tracking cloning attacks, and their countermeasures in respect of RFID, are explained in [23]. In RFID concern, authors in [24] introduced various tags, side-channel attack, timing attack, and briefly explained a protocol named "An Optimistic Trivial RFID Authentication Protocol" (O-TRAP). A security framework for E-passports, medical information systems, and implant-based access-control types vulnerable application areas, provided in [25], evaluates the security and privacy risk based on RFID. K. Bu et al. [26] has classified the cloning attack and their countermeasures on RFID, proposed in the last 15 years. They have also proposed their cryptographic solution to prevent cloning. An ultra-lightweight authentication protocol for RFID tags is defined in [27], which is suitable to provide security in IoT objects. An RFID based lightweight mutual authentication scheme is proposed in [28], which is suitable for providing security in medical IoT objects. Thus lightweight approaches for securing the RFID can also be used for securing the IoT network, concerned with RFID.

2.2 Wireless Sensor Network (WSN)

On one step towards the IoT, WSN technology is an integral part. Without sensors, one cannot assume the existence of IoT. In the 1950s, the first WSN was introduced by the US Military to find and track Russian submarines. A program on Distributed Sensor Network (DSN) was also started by the Defense Advanced Research Projects Agency (DARPA) of the United States in 1980 [29]. This technology is working on frequency bands 315, 433, and 868 MHz in the European countries, 915 MHz in North American countries, and 2.45-GHz ISM frequency band. Typically, the sensors used in WSN are battery powered and are less secure. The continuous development of WSN technologies, wireless communication technologies, embedded systems, nanotechnologies, and optimization of the sensors makes it possible to develop smart systems, to monitor activities of human beings and other

activities continuously. Various standards used by the WSN technology are ZigBee, 6LoWPAN, ISA100.11a, OCARI, and Wireless HART. IEEE 802.15.4 physical layer specifications standards are similar for all standards [30].

A WSN network with a blackhole attack scenario is shown in Fig. 4. Here, initially, the malicious sensor node "A" detects the active route for the sensor's data transfer from the sender node "S1" to the sink node or gateway. Attacker node "A" recognizes the detection address and sends a Route Replay Packet (RREP) with the spoofed destination address, based on the significant sequence number and small hop count to a nearest normal sensor node "S2". This node "S2" forwards RREP packets to the sender node "S1". Hence the data is being sent from sensor node uses the new route, which goes via malicious node "A." These data drop by a malicious node. Thus, the communication occurs between the sender and sink nodes, in case of a black hole attack [31]. In normal conditions (without attack), the sensing data is collected by the sink node/gateway and forwarded to the end-user by accessing the infrastructure network of the Internet.

A scheme named Active Trust proposed in [32] generates the number of detection routes for reducing the attack success probability of a black hole attack. For securing the WSN network, the probabilistic risk assessment framework is defined in [33], for the sensor's cloud environment with the help of Bayesian networks. Another security approach using the route optimization algorithm for increasing the network lifetime, and protection of the weak WSN node, is proposed by [34]. For a large mobile WSN case, a protocol named Q-s composite [35] is defined for random pre-distribution of the classified material.

2.3 Web of Things (WoT)

Designing a network of "smart things" in the physical world in huge amount has become the aim of various research activities. The layered architecture is the same in both the cases for IoT and WoT. IoT is the hardware layer to connect everyday items to the Internet, while WoT is the software layer to connect them to the Internet. For developing smart things applications, WoT uses various web technologies, such as JavaScript, PHP, and Ajax explained in [36]. A survey on WoT security conducted in [37], points out the current limitations of security research. He proposed architecture for WoT with security, based on smart gateways as the ideal devices.

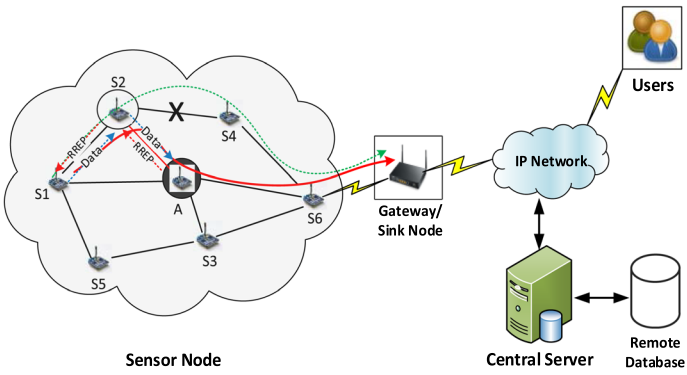


Fig. 4 WSN with Black hole attack specification [31]

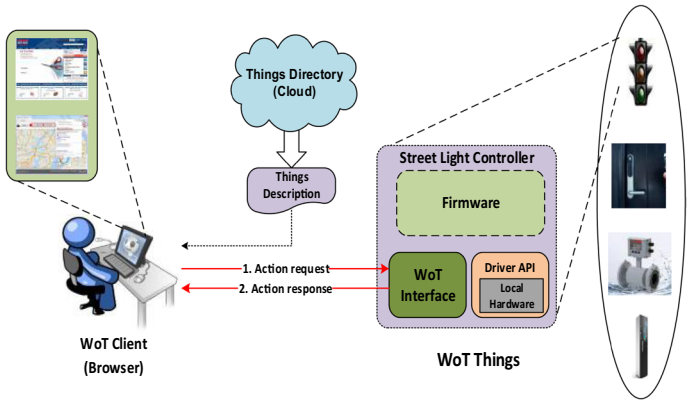


Fig. 5 Basic WoT things communication with WoT client

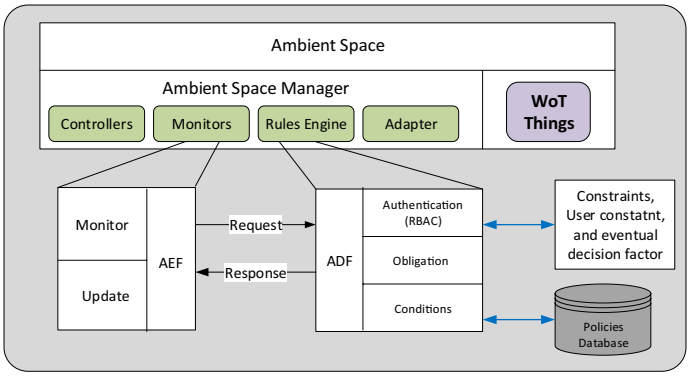


Fig. 6 Role-based access control/WoT architecture

Figure 5 shows the underlying communication architecture between WoT client and WoT things. The WoT client can be a web browser or an application on the user's system or smartphone. WoT Things (e.g., Street light controller) have a WoT network interface, driver's API, and firmware. Things description describes the interactions that can either be stored in the WoT device itself or any things directory stored remotely, such as the cloud server. When more secure access to the things description is required, the device supports itself.

For security consideration, initially, the WoT checks weather the WoT Client is talking with the correct WoT things or with some other network device. The WoT client must check the authenticity of the WoT thing device. Secondly, WoT things must verify the WoT client authentication before receiving the requests. Therefore, the mutual authentication process is performed between IoT client and IoT thing to supply credential information.

A Role-Based Access Control (RBAC) security architecture [38] is shown in Fig. 6. Its objective is to integrate the RBAC model with the WoT environment. A set of authorization rules are provided in this model to access any WoT Things/entities. Access control of the things resources is done centrally. It specifies a process, continuously working inside a trusted computer base named Reference Monitor (RM).

It is located inside the ambient space manager, compounded with two main facilities (1) Access Control Enforcement Facility (AEF) and (2) Access Decision Facility (ADF). AEF is situated inside the monitor section and ADF in the rule engine section. AEF and ADF interact with each other to check whether the access request is approved (yes) or blocked (no). AEF intercept each request coming from any WoT resource 'Things' and forwards it to ADF, before making any decision. ADF decision process depends on various decision factors, including hierarchal relationships, constraints, and policies database, and responds to the AEF. The rest of the process performed by the AEF would continue based on RBAC authorization permission.

2.4 Internet of Things (IoT)

As the name implies, it is the combination of three components, i.e., Internet, connectivity, and physical objects (things). IoT is the future of the Internet, in which every physical object is identified and access through the Internet. Various technologies (such as ZigBee (IEEE802.15.4), WLAN (IEEE802.11), Bluetooth/Bluetooth Low Energy (BLE) (IEEE 802.15.1), and Wireless Body Area Network (WBAN) (IEEE802.15.6)) are used to communicate the IoT data in the network [5].

2.4.1 Application Architecture of IoT

Figure 7 on this page shows the IoT real-time application architecture, broadly classified into three parts (a) Transmitting unit. (b) Communication channel and (c) Receiving unit. The transmission unit consists of various sensors, processors, and radio nodes. These nodes are further processed, and the cluster head is made. These sensor nodes are within the jurisdiction of the gateway, which assigns locally unique addresses to these IoT nodes within that particular LAN. This data flow through a proxy server and then goes to the cloud networks by using the Internet, where it uses a web socket to go to the cloud server. The cloud server analyzes the data, and various backend processes run in that cloud server. Based on that analytics and data processing, the actuation of devices takes place.

IoT technology supports applications such as smart homes, wearables, smart cities, smart grid, smart industry, connected health, smart security, transportation, and smart agriculture. These applications cover the maximum number of IoT objects, according to

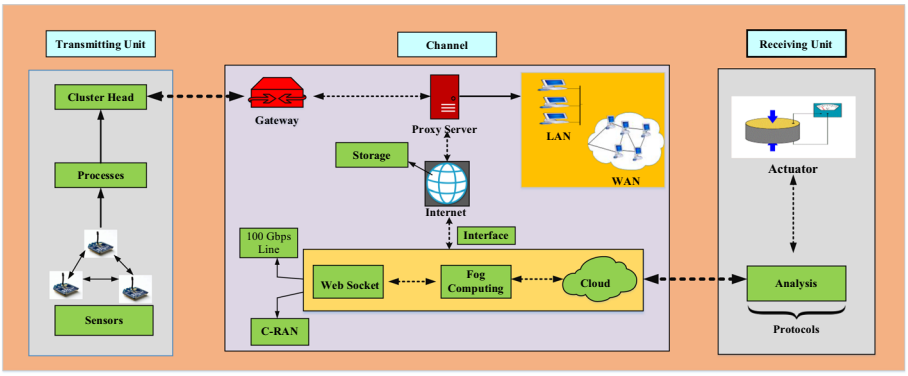


Fig. 7 IoT real-time application

iot-analytics.com. IoT provides a ubiquitous computing environment for increasing efficiency and reduces human effort through better knowledge of machines. It allows us to measure things which were not measurable earlier, or at least not in real-time, at a cost much lesser than other available alternatives.

2.4.2 Layered Architectures of IoT

IoT devices are always an attractive target for attacking. That's why security always becomes a challenging issue at the physical as well as the application layer. Due to the low cost and ultra-low-cost IoT modules, security solutions must be lightweight; otherwise, the cost of IoT devices would increase due to the complexity of the algorithm. Instead of securing a single unit of software or a single layer of IoT, we require to secure the entire IoT system. Three layers of security architecture have been proposed in [39], consisting of application layer, transportation layer, and perception layer. It differentiates various security issues based on this layered architecture. Authors in [40], defined Service Oriented Architecture (SOA) for IoT middleware and divided IoT Architecture into 5 sub-layers (application layer, middleware layer, Internet layer, access gateway layer, and edge layer) and also give the overview on the applications and various challenges on IoT. From the perspective of industry, [41] has introduced the background and some industrial applications of IoT. Service-oriented Architecture (SoA) of IoT defines the IoT as a well-defined simple subsystem. It divides the architecture into four sub-layers defined as an interface layer, service layer, network layer, and sensing layer. A five-layer architecture defined in Fig. 8 consists of the following layers.

2.4.2.1 Object Layer It is the lowermost layer. It may also be called a perception layer or physical layer. Different types of sensors like RFID, barcodes, infrared sensors, and other

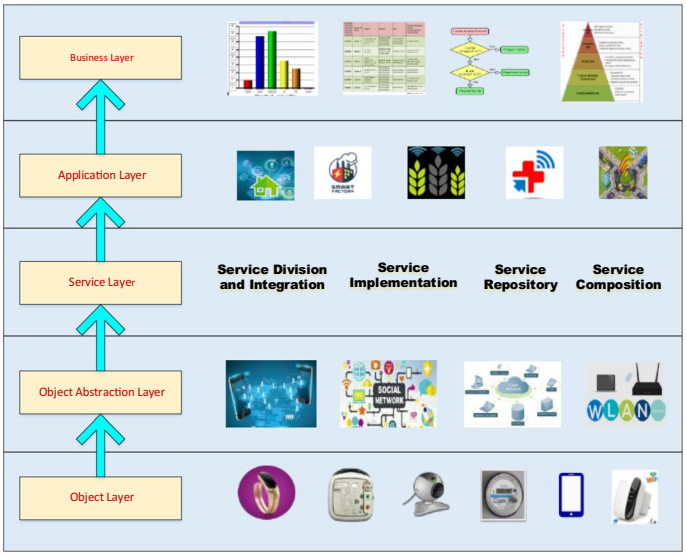


Fig. 8 IoT 5 layer architecture

sensor-enabled physical objects come under this layer. This layer collects the data of sensors and sends it to the upper layer.

2.4.2.2 Object Abstraction Layer This is the second layer in IoT architecture. It may also be called as the network layer. This layer abstracts the data of the object layer and transfers safely to the service management layer by using various communication technologies such as cloud computing, fog computing, WiFi, GSM, and LTE.

2.4.2.3 Service Layer The third layer of this architecture is the Middle layer of IoT architecture design. This layer manages and processes the data received from various heterogeneous networks. Services division and integration, service implementation, and provide services using a service repository to the upper layer. It works as a service platform to the upper layer.

2.4.2.4 Application Layer It gives the service to the customers based on their request for various applications of IoT such as smart home, smart healthcare, smart agriculture, smart industry, and smart grid.

2.4.2.5 Business Layer The uppermost layer of the IoT framework is a business Layer. It is also called the management layer. This layer is responsible for developing a business model, flowchart, and graphs. These are based on the data coming from the application layer. It helps in making future business strategies and planning for the growth of the organization.

3 IoT Security Matrix and Possible Attacks

With the growth of IoT in the past few decades, Internet traffic is increasing, and issues related to security are also increasing gradually. To address these issues, much research has been carried out by the industry and academia, such as resource allocation, lifetime enhancement in the sensor nodes, and power optimization. However, few works are there on security issues. Paradoxically, there is no security matrix that can accurately evaluate cryptographic security in the IoT environment. It still requires a more precise definition of the security standards in the IoT environment.

3.1 Security Matrix and Possible Layerwise Attacks

The main goal of security is to obtain favorable results for the following matrices.

3.1.1 Attack Success Probability (ASP)

It is defined as the probability of attack by an attacker, by which he can successfully achieve his attacking goal. In respect of IoT objects, there is a probability of compromising that object successfully [42]. If we consider any transmission network, ASP is the probability of compromising the target by affecting all the links (routes) that are used to connect the device with the network.

3.1.2 Attack Cost (AC)

It is the costing to the attacker for successfully achieving the attack goal. For any IoT object case, the metric is the costing by an attacker to compromise that object. The value of the attack cost depends on the node or object position on the IoT network [42].

3.1.3 Attack Impact (AI)

It is an effective loss done by an attacker to achieve his aim. This effective loss is the loss in terms of other previous basic metrics like availability, Integrity, and confidentiality. In the case of a single node, AI is the loss caused by an attacker to perform a successful attack on that node.

3.1.4 Mean-Time-to-Compromise (MTTC)

In IoT/NB-IoT network or any IoT object, MTTC is the value of average time consumed by an attacker to successfully compromise the node/network.

3.1.5 Secrecy Capacity (SC)

The difference in channel capacity $\left(C_{bs}\right)$ between the link established from source to destination in the normal condition and channel capacity (C_{ed}) of link affected by eavesdropper or intruder is known as Secrecy capacity $(C_{Secrecy})$ of the channel.

$$\text{i.e} \quad C_{Secrecy} = C_{bs} - C_{ed}.$$

3.1.6 Secrecy Outage Probability (SOP)

This term is used to characterize the secrecy performance of the communication system in terms of probability. The SOP is the probability that the secrecy capacity at a particular instant is less than a predetermined threshold secrecy rate. NB-IoT device's security will not be guaranteed to spoof the information, and hence, that system is said to be in an outage; otherwise, it is secured.

Figure 9 distributes the various possible security attacks on IoT as well as NB-IoT, layer-wise in 3 layers and 5 layers. These attacks break the device's security at a physical level, communication security at the network level, and management or application security at the application level. The definition of these attacks and their possible countermeasures are explained in Table 2.

3.1.7 Algorithms/Techniques for IoT Security

For securing the IoT device's data and communication networks, various algorithms proposed in recent years are described in this section in brief. These IoT security techniques focus on the small size, lightweight, efficient methods/algorithms. Various IoT techniques given in the table provided on the next page are related to NB-IoT, cybersecurity, fog-cloud-based IoT Networks. The pros and cons of these techniques are mentioned in the corresponding column.

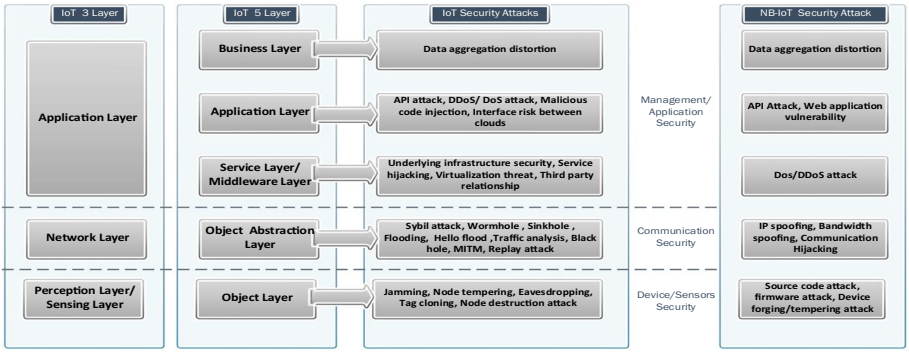


Fig. 9 Layer wise possible security attack

Singh et al. [61], combined symmetric and asymmetric key encryption and proposed hybrid lightweight techniques. Sedjelmaci et al. [14] used a simulator for achieving high detection accuracy. For Mobile IoT, Cheng et al. [15] introduced various patching techniques for blocking malware in IoT nodes. For narrowband IoT, Yang et al. [62] proposed an algorithm to secure traffic offloading for scenarios of single and multiple smart devices. Another hybrid algorithm has been given by Safi et al. [63] to improve the security of IoT. [64], proposed the HEIGHT algorithm to optimize energy requirement and hardware resources. For cloud and fog based networks, Shen et al. [65] gave a game-based strategy for detecting the malware. On the next page, Table 3 shows the security algorithms related to IoT.

3.1.8 Major Challenges in IoT

In IoT, most of the researchers are working to resolve the issues/challenges which will make the future IoT devices more reliable, standardize, secure, and compatible with another device. IoT applications cover the entire field related to our life. Everyone's identity is available for all, due to which in the current age of social networking IoT related device's data is always available for a robust security attack. There is no perfect secure prone architecture available in IoT networks, hence designing the standardized security architecture is a big challenge. NB-IoT technology is based on LTE technology, whereas some features of its specifications deemed unnecessary for LPWA needs have been stripped out. Due to this, NB-IoT is capable of providing unique advantages that other technologies like 2G, 3G, or LTE cannot achieve or could only do so at enormous cost. So, only NB-IoT gains its capability of long battery lifetime, deeper indoor coverage, and low module cost. In short, NB-IoT provides a bridge between IoT and power-optimized networks, i.e., it can solve the problem of energy consumption. The following are the significant challenges listed in tabular form, on which researchers and standardization committees have been working. IoT challenges are described in Table 4, and Fig. 10 shows it diagrammatically.

Table 2 Layerwise IoT/NB-IoT security attack

S. no.	Layer	Available attacks on IoT devices	Definition	Countermeasures	Refs.
1.	Business Layer	Data aggregation distortion	After collecting the data, the device sends it to the base station for further processing. An eavesdropper may distort (modify) this data, to be aggregated	Data integrity protection mechanism	[43]
2.	Application layer	API Attacks/Interface risk between clouds	API consists of a set of protocols and tools, for developing a software application. A poorly designed Application Programming Interface is often subjected to this type of attack. In IoT, the cloud service provider provides a set of API, that a user uses to interact with the clouds	The cloud service provider interfaced security model should be analyzed carefully Provides high Authentication and access control Understands the dependency chain associated with API	[44]
3.		DoS/DDoS attack	It is the most dangerous threat to IoT devices and networks. In this attack, the network becomes down due to a massive number of useless requests. It consumes the network resource due to which legitimate node does not respond to the request. Some DoS attacks, like Teardrop attack and Ping of Death, exploit the limitations in the TCP/IP protocols	Recognize the signs of a DDoS attack as early as possible DDoS mitigation plan by using a hybrid approach Introduce extra filter to inform the routers about packet drop from obvious attack source	[45]
4.		Malicious code injection attack	An attacker determines the system configuration to create Malicious/false measurements in the IoT network. It allows the attacker to bypass the security in the network	Estimation model Similarity check Testing before installation	[46]

Table 2 (continued)

S. no.	Layer	Available attacks on IoT devices	Definition	Countermeasures	Refs.
5.	Service layer	Underlying infrastructure security/service Hijacking	This type of security attack is performed in the lower layer of IoT services, i.e., Platform as a service (PaaS). The service provider is responsible for the security of this layer. Developer builds a secure application for the IoT device, but the security of these devices remains vulnerable due to the lower layer, due to which the services of this layer may also be hijacked	Fragmentation redundancy scattering	[43]
6.		Virtualization threat	The virtualization process allows the virtual machine to run different applications. It creates new opportunities for the attacker due to an extra layer that must be secured	Using the HyperSafe approach which gives hypervisor control-flow integrity	[43]
7.		Third-party relationship	When two or more than two data sources are combined, it increases data and network security issues. Platform as a service provides third-party web services components, called a mashup	Encryption of source data	[47]
8.	Object abstraction layer	Replay attack	In this, the attacker intercepts the message and retransmits this message multiple times, to consume the resource at the sensor	Introduce timestamp Implement the secure session key agreement	[48]
9.		MITM attack	In this most general attacking methodology, the attacker observes and interprets the information transfer between the IoT devices and gateway. After intercepting, the attacker can easily inject his information in the communication channel	Install and configure the firewall properly Update software regularly from trusted sources Use efficient encryption method between client and server and SSL certificates	[49–51]

Table 2 (continued)

S. no.	Layer	Available attacks on IoT devices	Definition	Countermeasures	Refs.
10.		Sybil attack	In this type of attack on IoT devices, attackers show itself as a legitimate user, although it manipulates fake identity, and thus it uses pseudo identities to compromise the effectiveness of the IoT	Use comprehensive comparisons for detecting mobile Sybil By using Sybil detection techniques based on the Social graph (SGSD) or behavior classification (BCSD)	[52]
11.		Flooding attack/hello flood attack	In this attack, the flood node transmits a large number of bogus data packets to all other nodes by establishing a route with all nodes in a network. These bogus packets can cause the failure of the network, and it is tough to identify the flood node also	Checking each node at regular interval of time with the help of a counter If any node in the network does not get a reply within a particular time threshold, the sender should be treated as the attacker	[53]
12.		Black hole attack	In this, the attacker node shows that the shortest path to the destination node passes from itself. Thus, the attacker node (black hole) attracts all the traffic towards itself	Routing access restriction False routing information detection	[54, 55]
13.		Traffic analysis attack	It this passive attack, the attacker analyzes and examines the communication patterns between IoT entities in a system	Encryption E-patterning and decentralization De-patterning and decentralization	[55]
14.		Wormhole attack	In the wormhole attack, first, the attacker node captures the packets from one place of network and then sends it to any other distant located place. It is easy to launch	Wormhole detection	[54, 55]

Table 2 (continued)

S. no.	Layer	Available attacks on IoT devices	Definition	Countermeasures	Refs.
15.		Sinkhole attack	In a sinkhole attack, the attacker node reflects the other nodes by showing its false routing information. By this, it attracts the network's traffic towards itself. It allows an attacker to redirect a system to a potentially malicious destination	Using cryptographic methods for protecting the network Make the restriction to each node with a certain threshold on the flow of data	[56]
16.	Object layer	Jamming attack	IoT network is vulnerable to jamming attacks, which could make IoT devices, deny the provide services to legitimate user, due to malicious radio jamming	The proposed algorithm can find a mixed-strategy Nash equilibrium of the Blotto game Detect and sleep Route around jammed regions	[57]
17.		Device/node capture/tampering attack	This attack occurs when sensor nodes/devices are not physically secured. In it, the attacker makes changes in the device in the form of program code or hardware circuits, due to which security of the device is compromised	Hide or camouflage nodes Tamper-proof packaging	[58]
18.		Eavesdropping attack	In this attack, eavesdropper interprets the data transmitted from the base station to IoT nodes. This captured data is used by an eavesdropper as input for a future attack. In the case of NB-IOT, a smart energy meter attacker intercepts the information about energy consumption. When it is negligible, he understands that no one is in the house, and steals the goods	Using a cryptographic algorithm Isolation, to prevent sniffing Access restriction	[55]

Table 2 (continued)

S. no.	Layer	Available attacks on IoT devices	Definition	Countermeasures	Refs.
19.		Tag cloning	In this attack, the attacker spoofs the identity of the RFID tag and clones it. The attacker uses this cloned tag in place of the original tag and replaces this cloned tag, with expensive items	Tag authentication algorithms	[59]
20.		Node destruction attack	Generally, the more dangerous form of node tampering, in which the node is physically destroyed or disabled. In the edge node case, the physical attack causes permanent destruction of the node	Preventing them physically, from unauthorized access	[55]
21.		Firmware attack	In this attack, the illegitimate user installs a malicious firmware on the IoT device and controls the device located at a remote place	Secure this attack by root access on IoT device system	[60]

Table 3 Algorithms/techniques proposed for IoT/NB-IoT security

References	Algorithm/technique proposed	Objective	Outcome	Pros(P) and Cons(C)	Year
[14]	Lightweight anomaly detection technique	The main objective of the work is to reduce the false-positive rate and energy consumption to achieve High detection accuracy	Using the TOSSIM simulator, the author achieves the objective	P: The technique consumes relatively less energy, compared to relatively other hybrid detection algorithms C: Suitable only for low resource IoT devices	2017
[62]	SolTPM	To find the optimal pairing between the smart devices (SD's) and access points (AP's), with secrecy provision for NB-IoT Systems	In a single-SD case, it effectively reduces the total power consumption In multiple-SD's and Multiple AP's, case, performance to optimal for SD-AD pairing with multiple parameters	P: This algorithm can help to improve the secure throughput, offloaded to the AP's C: Results are based on the limited number of SD's and AP's	2017
[15]	Traffic-aware patching	The main objective of this scheme is to block the IoT botnet masters and malicious sites, instead of securing important infrastructure links between the intermediate nodes and IoT devices	Proposed various other patching strategies like: • Patching by Path-Based Traffic Patterns • Various Importance Metrics for Intermediate Nodes • Transfer Learning for Optimal Patch Time	P: A useful technique for blocking malware intermediate node, via patching and restricts the damage C: Technique does not give an adequate mathematical model for predicting the malicious node	2017
[63]	HAN Algorithm	The proposed Hybrid encryption algorithm, which is the combination of asymmetric key and symmetric key algorithm, reduces the implementation time for IoT devices	The algorithm uses less memory, and implementation time is much lesser and reduced as compared to AES and RSA	P: Reduces encryption and decryption time, i.e., speeds up the calculation C: The algorithm uses multiple cryptographic techniques	2017

Table 3 (continued)

References	Algorithm/technique proposed	Objective	Outcome	Pros(P) and Cons(C)	Year
[64]	HIGHT cipher	It aims to enhance the performance of the block cipher algorithm	This encryption algorithm optimizes the FPGA implementation of the HEIGHT cipher. It has presented various optimization design approaches and minimizes the hardware resource and energy required, including the scalar and pipeline ones	P: Enhances the performance twice as compared to a conventional design algorithm C: Number of gates increases to more than 40% from conventional design	2014
[65]	Optimal PBE-based detection algorithm	The objective of this detection algorithm is to maximize the intrusion probability and minimize the hardware resource and energy required including the scalar and pipeline ones	It improves the detection accuracy of ID SaaS. It reduces the false alarm rate and increases the intrusion detection rate. It suppresses the malware diffusion accurately	P: Reduces the malware diffusion accurately C: Not suitable for different malware scenarios	2018
[66]	Secure Internet of Things (SIT) Algorithm	Provides low-cost security algorithm	This 64-bit block cipher and the crucial 64-bit algorithm use a low-cost 8-bit microcontroller for encrypting IoT data. The memory utilization of the algorithm is lower as compared to various other standard algorithms	P: Numerically, it shows better results for 64-bit Block cipher and key size C: The algorithm is not scalable	2017
[61]	Hybrid Lightweight Algorithm (HLA)	Proposed an efficient authentication scheme for IoT System	It combines the lightweight symmetric algorithm and asymmetric encryption algorithms for IoT devices. The result shows that computation cost is lesser, as compared to other relative schemes	P: No need of timestamp. C: Not suitable for high resource constraints device.	2017

Table 4 Major IoT challenges with NB-IoT solutions

S. no.	Type of challenge	Description	Possible solutions	References
1	Security issues at a different layer	Security in NB-IoT devices at low cost, lightweight, and designing cost-effective, efficient algorithms, which is acceptable for all types of IoT communication, is one of the critical issues in IoT. In 3 layer IoT architecture, various security issues like Key management, Sensors tag security, routing protocol security at perception layer, GPRS, Network, Internet Security at Transportation Layer and service support platform security, cloud computing platform security, etc. are at the Application Layer	As it is the primary concern of this paper, the development of the low resource, lightweight authentication schemes, or game theoretic-based approach, is a possible solution Blockchain coding can also be a solution in the case of NB-IoT One most favorable solution to these types of challenges is to develop cross-layer security techniques	[39]
2	Heterogeneity	Heterogeneity of IoT devices is also an issue for managing the different types of applications, environments, and a large number of devices in current scenarios. Heterogeneity may occur from a different perspective, like in topology, technology, the protocol used, etc. Co-operation between millions of IoT devices distribute over the Internet is also a big challenge. In other words, it can be said as global heterogeneity	Developing a user interoperability framework for working with various types of devices, which can coordinate and interoperate between thousands of distributed devices	[67]
3	Enormous heterogeneous data	IoT system generates a large amount of heterogeneous data, and it is different from the Internet. IoT devices generate trillions of gigabytes of data every year, so it is required to generate an efficient secure protocol to organize all this information. It would increase by ten times between 2013 and 2020, from 4.4 trillion to 44 trillion GB. This huge data can be treated as big data generation for the Internet. However, the IoT system generates heterogeneous data, and it is different from the Internet	It may be a good idea for implementing big data as a solution for solving this problem For handling huge amounts of different kinds of data, it requires a more comprehensive security solution. AI, Deep Learning based techniques will be better choices for resolving these data	[39, 68]
4	Standardization and Regulation	There is no standardized architecture of IoT defined by any certified regulatory authority till now. So it is a big issue to standardize and regulate various heterogeneous technologies, devices, and application interfaces used in IoT, which fulfill all the requirements	Initially, all supporting technologies related to IoT should be standardized, only then NB-IoT standardization can be possible	[69]

Table 4 (continued)

S. no.	Type of challenge	Description	Possible solutions	References
5	Compatibility	IoT devices are increasing in all directions and using various technologies, due to which deployment of extra hardware and software will be a problem	Due to the versatility of IoT, compatibility issues can be resolved by designing algorithms that support heterogeneous integration technology	[39]
6	Computational limitation	NB-IoT devices are very low-cost small devices. Finding a low-cost security solution is a significant challenge. The processing unit used in these NB-IoT enabled devices is not capable of processing large data size due to limited processing speed	In the case of NB-IoT and other low-cost devices, the development of an efficient lightweight protocol, having a small key size, may resolve it up to a certain level	[70]
7	Energy-efficient IoT	IoT devices are operated through the battery. Implant devices require long battery life. So it is a big challenge to find an energy-efficient security solution for devices	NB-IoT can resolve this problem up to some extent	[70]
8	Longevity	IoT enabled home appliances (smart TV, fridge, etc.) remain in functioning for a long time duration, even if their manufacturers may not	For improving durability, proper quality checks and services should be maintained	[39]

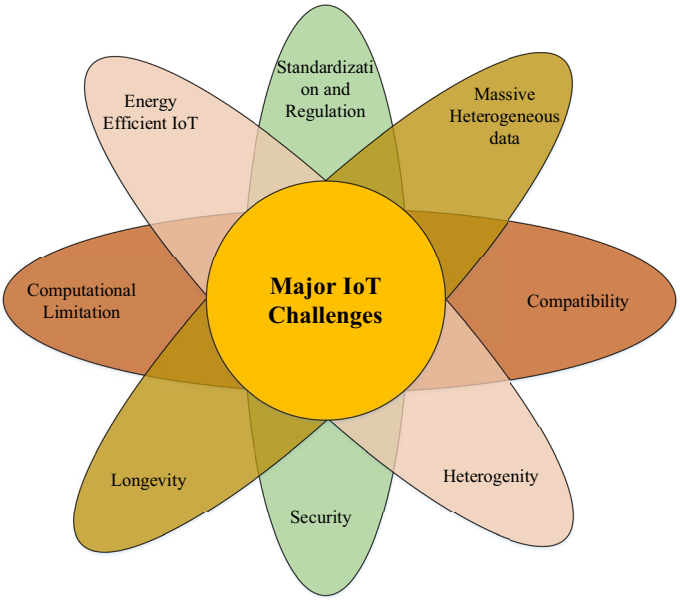


Fig. 10 IoT challenges

4 NB-IoT

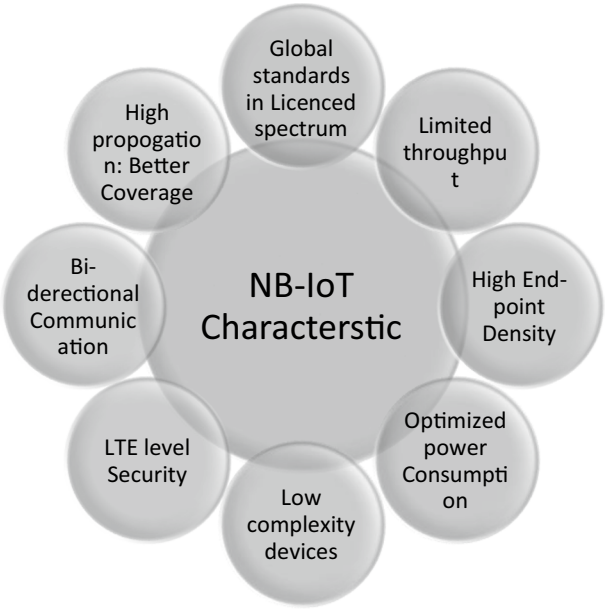
If we compare various LPWAN technologies, NB-IoT has drawn more attention from researchers and academia. Due to its features of High-end point density, low-cost, high indoor coverage, long battery life, and massive capacity, it is becoming the choice of most of the IoT devices, as shown in Fig. 11.

NB-IoT is operated at a low-frequency bandwidth of 180 kHz for both uplink and downlink and is suitable for low-cost devices. It offers a coverage range of 164 dB, and the latency of NB-IoT is around 10 s, i.e., it will target IoT devices that are located in the areas where signals are not good and are delay tolerant. Both IP and non-IP based data delivery are supported by NB-IoT. In the non-IP based data delivery, SMS service may also be used to deliver data, without using Internet protocol. As compared with other LPWAN technologies, the lesser spectrum is allocated for NB-IoT. The efficient use of the NB-IoT spectrum (i.e., resource allocation) is one of the key issues [71]. It reuses the existing LTE of GSM network structure. NB-IoT gives more flexibility for the deployment; hence, it is suitable for deploying the 5G network [72].

4.1 Operation Modes

NB-IoT can work in three operation modes, as shown in Fig. 12. Based on the available spectrum and use cases, the operator selects the most suitable operation mode to satisfy its requirement [73].

Fig. 11 NB-IoT characteristics



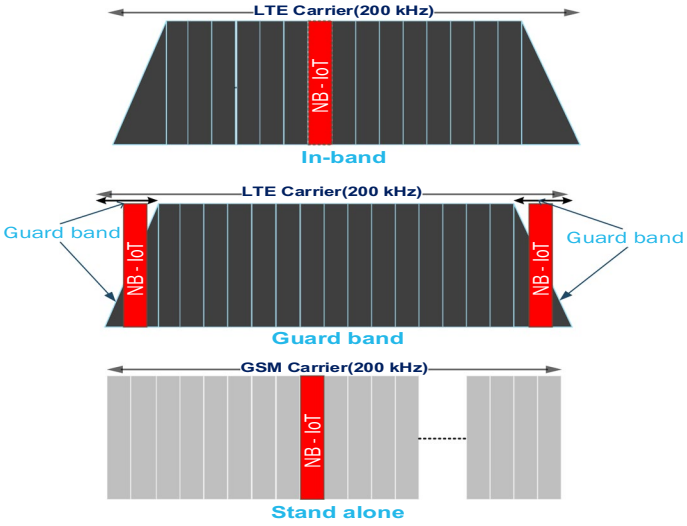


Fig. 12 NB-IoT operation modes

1. *In-band mode*: In the In-band operation technique, it utilizes 1 PRB of (180 kHz) the resources within the LTE carrier bandwidth.
2. *Guard-band mode:* In the guard band operation technique, NB-IoT uses the resource blocks within the guard band (edge frequency band) of the LTE carrier. It uses 200 kHz frequency band from the guard band.

3. *Standalone mode*. In it, NB-IoT can use one or more than one GSM (200 kHz) carriers and does not overlap with the LTE frequency band.

In NB-IoT uplink transmission, for a single tone, BPSK or QPSK modulation is used with 3.75 and 15 kHz subcarrier spacing. For a multi-tone case, the transmission is based on SC-FDMA with 15 kHz subcarrier spacing. For downlink transmission, QPSK modulation is used with 15 kHz subcarrier spacing with OFDMA technology.

4.2 Network Architecture

NB-IoT network architecture given in Fig. 13 is divided into four sections

1. *NB-IoT device* This layer is the physical layer consisting of the various NB-IoT sensor nodes which receive the commands and transmit the data to the base station.
2. *NB-IoT network* It consists of gateway nodes and base stations which transfer the NB-IoT device's sensing data.
3. *NB-IoT cloud* This layer receives, and stores sensing data from the base station and further performs data analysis. This platform may be a commercial platform like Amazon web services or any other end-user platform. NB-IoT Cloud platform consists of the Application Programming Interface (API). The main security issues concerned with NB-IoT originate in this layer.
4. *NB-IoT application server* It consists of various user applications, by which the user can interact with NB-IoT objects. The companies develop it according to their requirements. When any user requests for the data of any IoT device, this request will go through the NB-IoT cloud platform in the form of an HTTP request, then it forwards the request to the NB-IoT device. According to the request, the device will execute and reply to the cloud platform. Further, the cloud platform sends this data to the application server.

5 Security Issues and Proposed System Architecture related to NB-IoT

There are various LPWAN technologies that have been proposed by various network operators. Out of them, NB-IoT and LTE-M both are licensed LPWAN technologies, standardized in June 2016, by 3GPP release 13. NB-IoT network supports to design IoT devices.

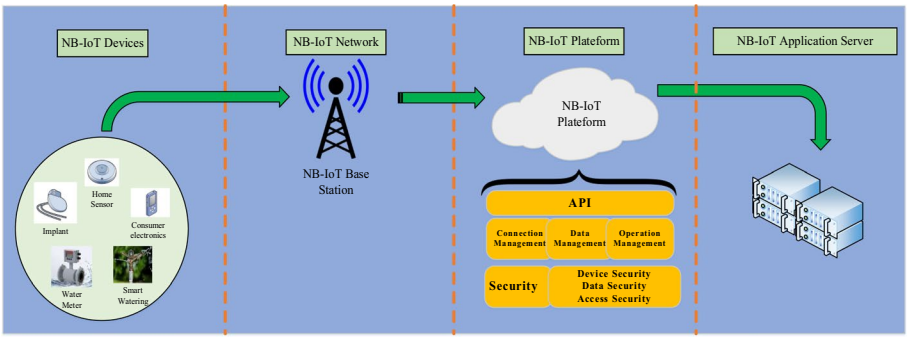


Fig. 13 NB-IoT network architecture

As IoT devices are small and cheap, security is neglected in most of the cases. That is the reason; the standardization is done by 3GPP, took no compromise when they defined this technology. NB-IoT devices have the capability of security directly from LTE, but NB-IoT is devised of any standardized security architecture. Some possible security attack scenarios based on applications and resource allocation are mentioned below, which can take place on NB-IoT.

5.1 Smart Home

We are living in a world of smart objects. These objects are not intelligent, just smart enough to be dangerous. Most of these devices are connected to the Internet, and hence IP enabled. These smart devices contribute to the pool of things that can be recruited into botnets or other platforms used for distributed attacks. These attacks make it more difficult to detect the source of the attack and also make it easier to overwhelm the target. In the past year, DDoS has become the attack of choice for attackers or blackmailers. In security attacks, IP spoofing [74] is the most common type of attack. Typically, this attack is performed over the stateless protocol named User Datagram Protocol (UDP). NB-IoT enabled devices, such as Digital Video Recorders (DVRs) and IP Cameras are the most vulnerable devices for the attack, in case of smart home security. There are approximately 1,20,000 IP cameras detected that are vulnerable to ELF_PERSIRAI.A, detected by Trend Micro Inc. Out of these vulnerable users, many users are unaware that their IP Cameras are exposed to the Internet.

5.1.1 Possible Security attacks

Smart home appliances and household IoT devices are easy targets to eavesdropper for compromising the security. These devices are typically secure and in the reach of the attacker. Fig. 14 shows some possible attacks that could impact on smart home objects/devices.

1. *Social attack* Social attacks may occur in many steps. In one of these, an eavesdropper investigates the victim's information, like which low-security protocol the victim is using and what is its trapdoor. After that, the attacker performs his action and gains the victim's trust. Then he takes the subsequent actions that break the security.
2. *Bandwidth spoofing* In this attack, we flood the communication channel to an extent, that legitimate traffic starts affecting the communication. While the bandwidth is being assigned to the NB-IoT device, there is more probability of acquisition of the bandwidth by the Attacker. Due to which communication between the base station and the device will be compromised. A possible solution to this type of attack is by using game theory [75].

5.1.2 Proposed Security Attack Architecture of NB-IoT Enabled Security Camera (Fig. 14)

In our proposed system model, we highlight mainly smart home security attacks and attacks on various sensitive inner implanted NB-IoT device. These devices consume very less amount of power, as they send and receive very less amount of data in a range of byte to few KB's to users. The battery life of these devices may extend up to 10 years.

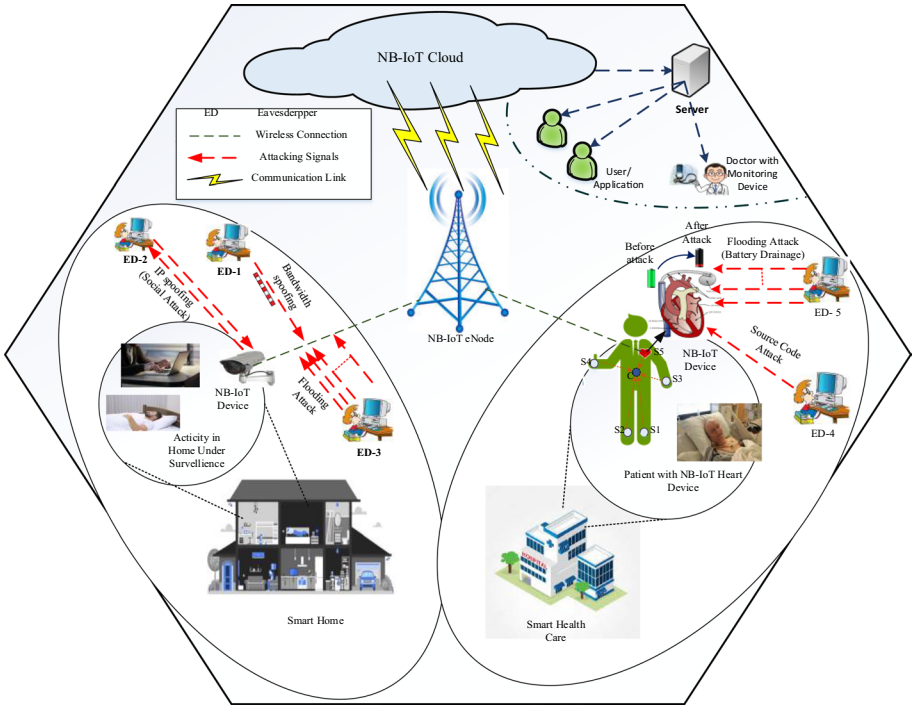


Fig. 14 Proposed system architecture of NB-IoT related attack

In smart home security, a smart security wireless camera is connected with the gateway, and using the bandwidth of NB-IoT is the crucial device to attack. Thief primarily attacks the device physically by switching off lights and may break it. If the attacker\eavesdropper (ED) is situated remotely, he can compromise that device in various manners like (a) IP spoofing, (b) flooding attack, and (c) Bandwidth spoofing, etc. As in IP spoofing, ED-2 may spoof the stationary device's (camera) IP packets, containing source (camera) IP address that is forged (spoofed) and may send the altered IP address to the base station. In the second case of flooding attack, eaves transmit a large number of requests to the device making it busy, due to which device is not able to respond to the request coming from a legitimate user (base station). In the third case of bandwidth spoofing attack, as the NB-IoT devices work on very low bandwidth, this type of attack is relatively easy in comparison with other technologies.

5.1.3 Mathematical Modeling

For physical layer Security, Shannon theory is used for analyzing the impact of eavesdropper in the NB-IoT device. First, we evaluate the secrecy capacity of the narrowband channel. In this section, we have derived the equation to calculate the secrecy rate and secrecy outage probability of the system model proposed above. Here we compare the complexity of the channel in an ideal situation with the secure transmission and after the attack of an eavesdropper. NB-IoT devices are working on half duplex-frequency division multiplexing operation mode with 60 kbps peak rate in uplink and 30 kbps peak rate in downlink

transmission. [76–80] define the secrecy rate and secrecy outage probability for different scenarios.

In the first case, Base Station (BS) allocates the channel to the NB-IoT enabled security camera, which is stationary and situated in a smart home. Let us consider a scenario in Smart Device (SD), i.e., that receives a signal y_{bs} from the base station, having the signal strength, i.e., SNR is Δ. Simultaneously, an ED has intercepted the signal and spoof the original signal (Δ) fully or partially, coming from BS to SD. ED has introduced the noise n_{ed}, due to which signal strength received by the NB-IoT enabled camera is now (Δ'), where ($\Delta \gg \Delta'$). The same phenomena are incorporated with the mathematical analysis is shown below.

For notation, we are considering that BS transmits the signal x_s.

The signal received from the base station is given by:

$$y_{bs} = \sqrt{P_{bs}} h_{bs} x_s + n_{bs} \tag{1}$$

where, P_{bs} is the average transmitted power from the base station, h_{bs} is the wireless fading channel coefficient and n_{bs} is the AWGN with variance σ^2_{bs}.

Simultaneously, the received signal from eavesdropper is given as:

$$y_{ed} = \sqrt{P_{bs}} h_{ed} x_s + n_{bs} + n_{ed} \tag{2}$$

Here,P_{bs} is the average transmitted power from the base station, h_{ed} is the wireless fading channel coefficient from ED to SD, n_{bs} is the Additive White Gaussian Noise (AWGN) and n_{ed} is AWGN due to eavesdropper signal, with variance σ^2_{ed}.

From (1), the channel capacity (BS- SD) can be written as:

$$C_{bs} = \log_2 \left(1 + \beta_{bs}\right) \tag{3}$$

where effective SINR:

$$\beta_{bs} = \frac{P_{bs} \left|h_{bs}\right|^2}{\alpha + \sigma^2_{bs}} \tag{4}$$

Here channel gain is $\left|h_{bs}\right|^2$, and α is interference due to the intruder.

From (2), the channel capacity C_{ed} has been affected by ED, and an intruder also inspects it. Hence channel capacity has been reduced as per equation is written as:

$$C_{ed} = \log_2 \left(1 + \beta_{ed}\right) \tag{5}$$

where effective SINR:

$$\beta_{ed} = \frac{P_{bs} \left|h_{ed}\right|^2}{\alpha + \sigma^2_{bs} + \sigma^2_{ed}} \tag{6}$$

With the consideration of a cooperative eavesdropping attack, there is n number of attacker attacks simultaneously. Hence the channel capacity for n eavesdropper cooperative attack is:

$$C_{edn} = \log_2 \left(1 + \beta_{edn}\right) \tag{7}$$

where effective SINR,

$$\beta_{edn} = \frac{P_{bs}\left|h_{edn}\right|^2}{\alpha + \sigma_{bs}^2 + \sigma_{ed_1}^2 + \sigma_{ed_2}^2 + \sigma_{ed_3}^2 - - - + \sigma_{ed_n}^2} \tag{8}$$

β_{edn} is SINR due to n cooperative eavesdroppers on the channel, $\left|\mathrm{h_{edn}}\right|^2$ is the channel gain and $\sigma_{ed_1}^2, \sigma_{ed_2}^2, \sigma_{ed_3}^2, \ldots .., \sigma_{ed_n}^2$ are the variance of n eavesdroppers respectively.

Secrecy capacity is denoted by the difference between the capacities of the base station channel and the eavesdropper channel. As the channel capacity has a non-negative value, therefore the secrecy capacity (SD–BS) in the presence of eavesdroppers is given by:

$$C_{Secrecy} = [C_{bs} - C_{ed}]^+ = [\log_2\left(1 + \beta_{bs}\right) - \log_2\left(1 + \beta_{ed}\right)]^+$$
$$C_{Secrecy} = \begin{cases} \log_2 \frac{(1+\beta_{bs})}{(1+\beta_{ed})} & \beta_{bs} > \beta_{ed} \\ 0 & \beta_{bs} \leq \beta_{ed} \end{cases} \tag{9}$$

i.e., Secrecy capacity is positive if the SINR of the base station is greater than the eavesdropper, and it becomes zero when eavesdropper's SINR is greater than the base station.

From Eq. (9):

$$C_{Secrecy} = \begin{cases} \log_2 \frac{(1+\beta_{bs})}{(1+\beta_{ed})} & \beta_{bs} > \beta_{ed} \\ 0 & \beta_{bs} \leq \beta_{ed} \end{cases}$$

Putting values of β_{bs} and β_{ed} from Eqs. (4) and (6) the equation becomes:

$$C_{Secrecy} = \begin{cases} \log_2 \frac{\left(1+\frac{P_{bs}\left|h_{bs}\right|^2}{\alpha+\sigma_{bs}^2}\right)}{\left(1+\frac{P_{bs}\left|h_{ed}\right|^2}{\alpha+\sigma_{bs}^2+\sigma_{ed}^2}\right)} & \beta_{bs} > \beta_{ed} \\ 0 & \beta_{bs} \leq \beta_{ed} \end{cases}$$

In the case of n collaborative eavesdroppers, the Secrecy Capacity of the channel is given by:

$$C_{Secrecy}^n = [C_{bs} - C_{edn}]^+ = \left[\log_2\left(1 + \beta_{bs}\right) - \log_2\left(1 + \beta_{edn}\right)\right]^+$$
$$C_{Secrecy}^n = \begin{cases} \log_2 \frac{(1+\beta_{bs})}{(1+\beta_{edn})} & \beta_{bs} > \beta_{edn} \\ 0 & \beta_{bs} \leq \beta_{edn} \end{cases} \tag{10}$$

i.e., in the above situation, in cooperative eavesdropping attack, when SINR of the base station is greater than the SINR of cooperative attacks of an eavesdropper, secrecy rate will be positive. Otherwise, it will be zero, and eavesdropper will compromise the system.

Now, Channel capacity becomes

Case-I When eavesdropper trapped the mail channel, additional noise added with the channel. The same has been reflected in equation (9).

Case-II In NB-IoT, operating devices are associated with low power, and if intruder spoofs the bandwidth using game theory against the valid user, then bandwidth spoofing plays a vital role in NB-IoT security issues because this attack directly affects the bandwidth assigned to the valid user (capacity assigned to the valid user). Let us assume that if λ is a factor associated with the bandwidth spoofing attack, then resultant capacity is reduced by C/λ, so in this case from equation (5) the channel capacity is

$$C_{ed}^{'} = \frac{C_{ed}}{\lambda} = \frac{1}{\lambda}\log_2\left(1+\beta_{ed}\right) \tag{11}$$

Case-III (protection phenomena) In the case of IPsec, an encapsulation phenomenon appears, so there is a tunnel between NB-IoT device (Camera) and the base station. So eavesdropping and bandwidth spoofing can be avoided.

$$C_{ed'}^{'} = \frac{C_{ed}}{\lambda'} = \frac{1}{\lambda'}\log_2\left(1+\beta_{ed}\right) \tag{12}$$

Hence the value $\frac{C_{ed}}{\lambda'} > \frac{C_{ed}}{\lambda}$, when $\lambda' > \lambda$, due to the protection of the spoofed channel by IPSec.

Secrecy Outage Probability Analysis

In this section, we find the secrecy capacity of the channel in terms of the Secrecy outage probability (SOP). This performance measurement is used to characterize the secrecy performance of the NB-IoT channel communication system. The SOP is termed as the probability that the instantaneous secrecy capacity $C_{Secrecy}$ is less than a predetermined threshold secrecy rate R_{sec} (i.e., if $C_{Secrecy} < R_{sec}$). NB-IoT devices security will not be guaranteed to spoofed information, and so that the system is said to be in outage; otherwise, it will be secured.

$$\mathcal{P}_{out}\left(R_{Sec}\right) = \mathcal{P}(C_{Secrecy} < R_{Sec}) \tag{13}$$

Equation (13) can be rewritten as

$$\mathcal{P}_{out}\left(R_{Sec}\right) = \mathcal{P}(\frac{\left(1+\beta_{bs}\right)}{\left(1+\beta_{ed}\right)} < 2^{R_{Sec}}) \tag{14}$$

The operational significance of this definition of outage probability is when we set the secrecy rate $R_{sec} > 0$.

Let us assume that the capacity of the eavesdropper channel is given by:

$$C_{ed}^{'} = C_{bs} - R_{Sec}$$

As $R_{Sec} < C_{Secrecy}$, eavesdropper channel is worse than base station channel i.e. $C_{ed} < C_{ed}^{'}$, so it will ensure perfect secrecy. Otherwise, if $R_{Sec} > C_{Secrecy}$, then $C_{ed} > C_{ed}^{'}$ and information is compromised.

In *Case-I* when additional noise is added by an eavesdropper, SOP comes from (14)

$$\begin{aligned}\mathcal{P}_{out}\left(C_{Secrecy}\langle R_{Sec}|\beta_{bs} > \beta_{ed}\right) &= \mathcal{P}(\beta_{bs} < 2^{R_{Sec}}\left(1+\beta_{ed}\right) - 1|\beta_{bs}\rangle\beta_{ed}) \\ &= \int_{0}^{\infty}\int_{\beta_{ed}}^{2^{R_{Sec}}(1+\beta_{ed})-1} \mathcal{P}(\beta_{bs},\beta_{ed}|\beta_{bs} > \beta_{ed})d\beta_{ed}d\beta_{bs} \\ &= \int_{0}^{\infty}\int_{\beta_{ed}}^{2^{R_{Sec}}(1+\beta_{ed})-1} \frac{\mathcal{P}(\beta_{bs}\mathcal{P}\left(\beta_{ed}\right)}{\mathcal{P}(\beta_{bs} > \beta_{ed})}d\beta_{ed}d\end{aligned} \tag{15}$$

Now since secrecy rate $R_{sec} > 0$

$$\mathcal{P}_{out}\left(C_{Secrecy}\langle R_{Sec}\middle|\beta_{bs} \leq \beta_{ed}\right) = 1$$

Considering case-II of bandwidth spoofing and case-III of game theory and encapsulation phenomena will be proposed for future work.

Let us assume that

C = C_{bs} → Capacity of the channel without attack
Cs = C_{ed} → Capacity of the channel in the presence of an eavesdropper

From Eq. (3)

$$C = \log_2\left(1 + \beta_{bs}\right) \tag{16}$$

From Eq. (5)

$$C_S = \log_2\left(1 + \beta_{ed}\right) \tag{17}$$

The ratio of C/C_S can be calculated as

$$C/C_S = \log_2\left(1 + \beta_{bs}\right)/\log_2\left(1 + \beta_{ed}\right) \tag{18}$$

n_{bs} is the Additive White Gaussian Noise (AWGN) and n_{ed} is AWGN due to eavesdropper signal, with variance σ_{ed}^2.

If $n_{bs} \leq n_{bs} + n_{ed} \rightarrow \sigma_{bs}^2 \leq \sigma_{bs}^2 + \sigma_{ed}^2$

So from Eqs. (4) and (6)

$$\beta_{bs} \geq \beta_{ed}$$

Hence from Eqs. (3) and (5) channel capacity of the eavesdropper signal is less than the channel capacity of base station.

$$C_{bs} \geq C_{ed}$$

$$\frac{C_{bs}}{C_{ed}} \geq 1 i.e. \frac{C}{C_S} \geq 1 \tag{19}$$

For example, if we have taken $\beta_{bs} = [3, 7, 15, 31, \ldots]$ and $\beta_{ed} = [1, 3, 7, 15, \ldots]$, then ratio of both capacity comes $\frac{C}{C_S} = [2.0, 1.5, 1.33, 1.25, \ldots towards\ 1]$ (Table 5).

5.2 Smart Healthcare

If we go towards smart healthcare devices, they are tiny in size and consume very less amount of battery power for transmitting the information to the end-user. Some of these device implants in the inner body of the human/animal and are very critical. If an eavesdropper sends a fake request to the device continuously, the battery power starts draining quickly, i.e., battery life is reduced from 10 years to a few days. It will make the patient's condition critical. Another attack shown in the system architecture is the source code attack, i.e., if the attacker changes the hardware source code anyhow, the device will not perform as usual and give wrong results, which can also result in severe problems with the patient. Figure 15 shows the small overview of attacks on health implants devices. Many

Table 5 List of symbols

S. nos.	Representation of symbol	Meaning of symbol
	x_s	Base station transmit signal
	y_{bs}	The received signal from the base station
	y_{ed}	Received signal at eavesdropper
	P_{bs}	Power at the base station
	h_{bs}	Wireless channel fading coefficient (BS-SD)
	h_{ed}	Wireless channel fading coefficient (SD–SD)
	n_{bs}	AWGN due to the base station
	n_{ed}	AWGN due to eavesdropper signal
	C_{bs}	Channel capacity (BS- SD)
	C_{ed}	Channel capacity after ED affection
	C_{edn}	Channel capacity of n ED cooperative attack
	β_{bs}	SINR from BS
	β_{ed}	SINR after ED affection
	β_{edn}	SINR due to n cooperative eavesdroppers
	$\lvert h_{bs}\rvert^2$	Channel gain due to BS
	$\lvert h_{ed}\rvert^2$	Channel gain due to ED
	$\lvert \mathrm{h}_{\mathrm{edn}}\rvert^2$	Channel gain due to n ED's
	σ_{bs}^2	Variance (base station)
	σ_{ed}^2	Variance (eavesdropper)
	$\sigma_{ed_1}^2, \sigma_{ed_2}^2, \ldots, \sigma_{ed_n}^2$	The variance of n eavesdroppers respectively
	$C_{Secrecy}$	Secrecy capacity (SD–BS) in the presence of eavesdroppers
	$C_{Secrecy}^n$	Secrecy capacity (SD–BS) in the presence of n cooperative eavesdroppers
	λ	A factor associated with the bandwidth spoofing attack
	$\mathcal{P}_{out}$	Secrecy outage probability
	R_{Sec}	Secrecy rate
	α	Interference due to the intruder

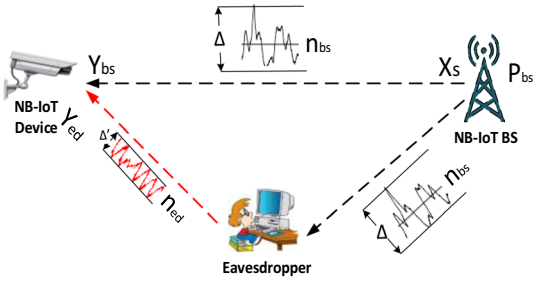


Fig. 15 NB-IoT device Case-I scenario

smart wearable healthcare devices use NB-IoT technology due to long battery life and deep indoor coverage features.

5.2.1 Proposed Healthcare Security Attack Architecture

In the first case, we consider another attack possible on the pacemaker device, i.e., the source code attack in which the code written on EEPROM is altered or erased so that it will give wrong information of the patient. These devices are implanted inside the human body or are wearable in the wrist or other body parts. Attacks on these type of devices are critical due to concern with the health. The scenario of these attacks is shown in Fig. 15. Attacks on healthcare monitoring devices come under this category.

Pacemaker, a medical heart implant device, delivers an electrical impulse to the heart muscles to regulate the beating of the heart. This pacemaker is programmed by a cardiologist to select optimal pacing modes for individual patients. This device consists of two main components [81]. The first one is the device controller monitor (DCM), and the second is the pulse generator (PG). DCM has a graphical user interface with three tabs, consisting of current pacemaker configuration, system default value, and patient information. All the information and parameters of DCM are written in EEPROM on the pacemaker board so that pacemaker can also operate in off mode without any intervention. The work of DCM is to: (a) review battery status, (b) program the system before implementation, (c) Evaluate ventricular and atrial lead signal amplitudes, impedances, and pacing thresholds, (d) set up appropriate parameters (e) test the pacemaker in the patient and (f) Interrogate the system.

A second most important part of the pacemaker is PG. Its work is sensing and generating the pulse signals as needed to keep the patient's heart beating. PG code divides into two parts: Hardware dependent and hardware independent. The first one has a device driver, timers, and the second one consists of a model used to verify the correctness of the pacemaker.

In the second case, an eavesdropper (ED-5) sends a large number of request signals to a pacemaker. As a result of which, the battery drains rapidly, and the patient's organs information will not transfer to the respective caretaker. This type of flooding attack may generate a problem for the patient.

5.2.2 Proposed Healthcare Attack

1. *Source code attack* Source code attack is among the deadliest attack on NB-IoT operated healthcare devices. In this attack, the device code written on PROM, are the main target of the attacker. This code can be changed by the programmer (attacker) partially or erased, and a new code can be written on the compromised device. Details of this attack have been provided in the previous section.
2. *Battery drainage attack* Another attack possible on the tiny size, healthcare devices, is the attack on battery power. As the battery life of the NB-IoT device is more than 10 years, its battery drains very slowly. In this type of attack, eavesdropper sends a large number of request messages to the device. The device responds according to request, which consumes much energy, i.e., battery usage is very high. As a result, the device's battery drains rapidly. It will create a critical condition for the patient, who implants this healthcare device.

5.3 Smart Agriculture

Smart agriculture *is* not as popular as smart health or smart consumer connected devices. Smart agriculture consists of crop Management, Cattle monitoring in dairy form, climate monitoring, greenhouse automation, etc. Attacks on NB-IoT enabled agriculture system monitoring devices are not as critical as human body implant devices, but it will affect crop production, cattle health, fish farming, etc. Somewhere it is also called e-farming. IoT technology can support precision agriculture, whose aim is to provide maximum return on investment in agriculture with the help of soil ph detection/humidity/temperature sensors. Usually, the agriculture system runs on an unmonitored network, due to which attacks attempted on it go unobserved. An eavesdropper can easily access the irrigation control system, pesticide administration, Cattle health information and manipulate it, without the farmer knowing. These are some attacks that are possible in the agriculture system.

5.4 Attacks Based on NB-IoT Resource Allocation

It is a big task to allocate proper resources to the NB-IoT object so that it operates without any external intervention. The allocation of the resource is performed in a manner to minimize the maximum risk, controlling the range of operation of the attacker. There are various types of possible risks/attacks that reduce the effectiveness of their activity.

5.4.1 Possible Resource Allocation Attacks

1. *Resource exhaustion* It happens when the NB-IoT base station does not control the amount or size of resources properly that are requested by the object [82]. By which more resources are utilized, intended by the resource allocator. These limited resources may be a memory, file system storage, or processing unit. If this resource allocation is monitored and triggered by an attacker and the amount of the resource is not controlled, the attacker can consume all the available resources and can perform DoS attack, due to which legitimate devices may not be able to use the resources appropriately and face the problem to access it. For example, memory exhaustion attack against an application used by NB-IoT object could slow down the application as well as the resource allocator operating system.
2. *Selective forwarding attack* In this attack, attacker nodes act like normal nodes and selectively drop the packets. These drop packets may be random, and sometimes it is impossible to identify such attacks. In [83], the authors simulate the selective forwarding attack for more than 500 nodes. These nodes are not protected for a long time duration when the defense strategy is changed, and the security resource that maximizes the risk is removed.
3. *Bandwidth spoofing* As already discussed previously [75], it is one of the significant resource allocation attack possible due to the limited amount of bandwidth (180 kHz) available for NB-IoT device. This bandwidth allocation attack possibility is high at the time of the bandwidth assignment.
4. *DDoS attack* Distributed denial of service [45] is a significant threat in resource allocation for IoT/NB-IoT. As discussed in Table 2, in this attack, the NB-IoT device refuses to respond to the request coming from the legitimate user due to the non-availability of the resource. Earlier, this attack was performed by underground attackers. DDoS attacks

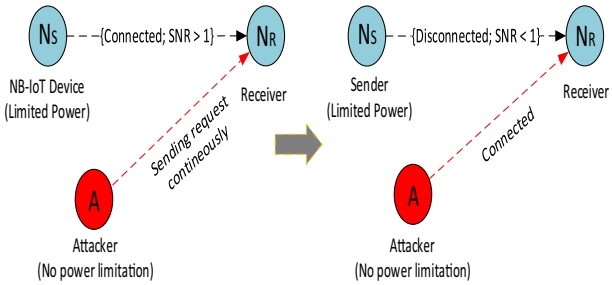


Fig. 16 Node failure attack

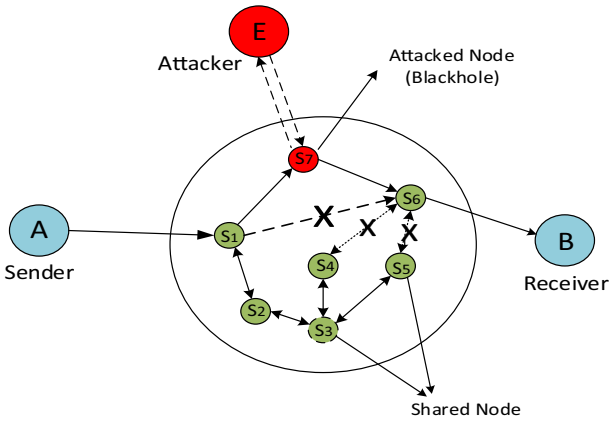


Fig. 17 Shared node attack

on unsecured IoT devices are doubled every year, as per the report published in 2017 by a security firm Corero. Mirai, the most successful DDoS attack, occurred in September 2016. It almost disabled a website with 620 Gbps of network traffic attack.

5.4.2 Proposed NB-IoT Based Resource Allocation Attacks

1. *Node failure attack* At the time when sender node transfers the information to the receiver node, an outside attacker sends multiple requests to the sender for data, due to which the sender node's Signal to noise ratio (SNR), which is greater than one, comes down to less than one. To increase the SNR, the sender node increases power.

   This process continuously runs between the sender, attacker, and transmission channel. After a certain period, due to limited power constraints of NB-IoT device, the sender power is drained out, and the node becomes down or fails to transmit the data signal. Fig. 16 helps to understand the node failure attack.
2. *Shared node attack* This resource allocation attack is possible *when* sender A is not able to send the data from S_1 to S_6, and hence sends the data through node S_7. This mediator node S_7 is known as a shared node. As shown in Fig. 17, among these shared nodes, the attacker acts like a black hole and shows themselves that it provides a better transmission path to send the data at the destination node with good channel conditions. While in reality, the attacker node captures the packets and after alteration, shares these packets to other nodes or with the destination node. This attacked node shows to other adjacent nodes that it is a reliable node and can forward the adjacent node's data efficiently to

the destination node, that it captures the network data and forwards the altered data to the receiver node.

3. *Synchronization attack* In synchronization attack, transmitter node N_A synchronizes with the receiver node N_B by sending a timestamp with the data packet, as shown in Fig. 18.

In between this communication channel, an attacker C captures the data from Node N_A and forwards it to the receiver N_B via another attacker D. However, the data sent via D does not synchronize with the receiver N_B and discards it in starting, due to synchronizing with the sender node N_A. Response time of the attacker node D is less than N_A because hop count associated with N_B is less than N_A. Hence, the response time of D is less than N_A. So, after a certain period, D synchronizes with N_B instead of N_A.

5.4.3 Protections Approach for Resource Allocation Based Attacks

More than 25% of the cyber-attacks will be on the connected devices till 2025 (according to the report on IoT security by Digital security). These connected devices may be using any of the IoT technology. Among these technologies, NB-IoT connected devices will also get affected by the attackers. However, NB-IoT provides LTE level security. Various protection strategies like game theory, artificial intelligence, deep learning may be some good sources to secure data communication between low resourced NB-IoT devices. Rullo et al. [83], proposed a security model using Pareto optimality solution, by which the probability of a successful attack is minimized. He also provides a resource allocation plan for different large-scale network topologies. Another game theory oriented security approach using a Nash equilibrium is defined in [84]. In the game model, the defender's objective is to maintain the highest security of the whole IoT system, through the selection of respective detection threshold value, while the attacker's goal is to optimize the attack on the device/node with limited attacking resources. Article [85] contributes the Machine Learning (ML) based on an unauthorized IoT device's detection approach. This experimental technique is based on supervised ML, and provides approximately 99% accuracy on test data results, collected from 17 IoT devices with 9 different types of devices.

Another ML-based IoT security enhancement technique, named RF-PUF proposed in [86], uses the preexisting asymmetric radio frequency communication framework, so it does not require extra circuits for physically unclonable function (PUF) generation. He employed an Artificial Neural Network (ANN) as a learning engine. Simulation results employ 99% accuracy using supervised learning. [87] provides a deep learning based approach for detecting Internet of Battlefield Things (IoBT) malware and junk code

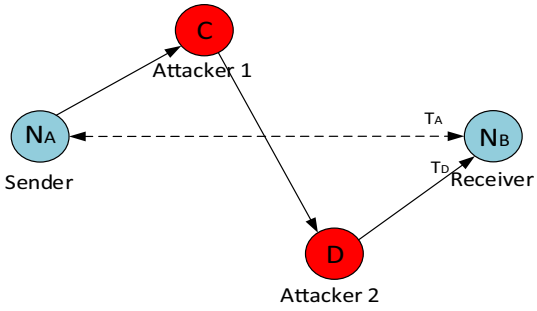


Fig. 18 Synchronization attack

detection. He proposed a method consisting of two-phases. One is the OpCode-Sequence Graph Generation phase, and the other is the Deep Eigenspace Learning phase.

The security issues in NB-IoT can be dealt with blockchain coding because NB-IoT operation is based on energy efficient optimization. In a real-time scenario, the same group of applications demanded by IoT devices can be grouped, and security techniques/protocol can be applied on the basis of grouped numbers (behavior or types of IoT devices). Blockchain techniques are beneficial in such problems because, through blockchain techniques, tunneling phenomena can be applied based on the group instead of IoT devices secured separate channels. Hence this technique is beneficial for energy efficient resource allocation. As per the report produced in i-scoop.in, 20% of IoT deployment is based on the basic blockchain services till 2019.

6 Conclusion and Future Work

This paper provides an extensive survey of security issues related to IoT and NB-IoT technologies. At the same time, this paper provides a bridge between IoT and NB-IoT. Security issues play a vital role in the current IoT network. With the consideration of this as a researcher and academia, we have focused our work related to security issues in NB-IoT like social attack, health care attacks, bandwidth spoofing attack, IP spoofing attack, etc. To provide the real-time deployment of NB-IoT, we have addressed the resource allocations with mathematical analysis, and also different algorithms and techniques have been incorporated with the consideration of security issues in NB-IoT. Possibilities of security issues in NB-IoT architecture have been proposed with a consideration of real-time applications and also formulated, how we can overcome these possible security problems.

Artificial Intelligence-based optimizations will provide an excellent platform to protect spoofing attacks for future NB-IoT real-time deployment. It is based on adaptive prediction techniques for spoofing attacks by using data mining or stochastic process. The accuracy of this type of cross-layer optimization is very high as compared to general prediction scenarios.

Acknowledgements The authors thankfully acknowledge the support provided by SMVDU-TBIC and 5G & IoT Laboratory, School of Electronics and Communication Engineering at Sri Mata Vaishno Devi University, Katra.

Appendix

IoT Security Projects

Under various research projects, the most prominent research and innovation programs are funded by the European Union named Horizon 2020. The funding of this program is 80 billion euros and available for the 7-year duration (2014–2020) [88]. Stanford, University of Michigan, and UC Barkley are collaboratively working on a 5-year project named Secure Internet of Things Project (SITP). It was started in September-2016 to research fundamentally new and better ways to secure the IoT and make them easy to use. They are working in this area. Table 6 shown below describes the various projects running currently worldwide. Most of the projects aim to provide end to end secure transmission between devices, implementing security techniques, and working towards the smart city. Various IoT projects running in European countries are working towards smart business, smart country, and removing various security vulnerabilities.

Table 6 Current ongoing NB-IoT/IoT security-related activities

S. nos.	Project name	Aim of research	Area of research	HTTPS location
1	stalkIT	This project rovides the low cost and long life asset monitoring systems	The project is based on LPWAN technology, such as NB-IoT and LTE-M	https://cordis.europa.eu/project/id/887525
2	Mitigating IoT-Based DDoS	This project aims to lower the vulnerability of the system to automated distributed threats based on exploration	The project focuses on consumer and small business environments	https://www.nccoe.nist.gov/projects/building-blocks/mitigating-iot-based-ddos
3	ECRYPT-NET	The aim of the project is to find advanced cryptographic methods for IoT and cloud networks so that it will provide high-level security and improve the usability of the IoT devices	It helps to remove the disintegration of the advanced cryptography area. Device security is the main parameter to develop this technique. Its area is to maintain privacy and cybersecurity in Europe	http://www.ecrypt.eu.org/net/
4	MONICA	The project focuses on the deployment of a secure, cloud-based platform, and managing public security and safety of large crowds	Working for sound and security application of large scale crowds, for open-air cultural and sports events in the city	http://www.monica-project.eu/
5	SecIoT	The project aims to scale up the business towards the area of IoT security by implementing a disruptive innovative solution, that will definitively allow increasing its competitiveness and internationalization objectives	The area of this project is to provide cybersecurity to various IoT devices that are connected. It.is also working for various threat detection schemes for IoT devices to give adequate security to society	https://cordis.europa.eu/project/rcn/208832_en.html
6	ACTIVAGE	A part of this project is working for the ACTIVAGE secure interoperability layer, whose aim is to allow interconnecting heterogeneous IoT devices and provide dedicated attention to security and privacy	Working for smart living application for social and economic wellness, mainly in healthcare orientation	www.activageproject.eu/

Table 6 (continued)

S. nos.	Project name	Aim of research	Area of research	HTTPS location
7	SEMIoTICS	SEMIoTICS aims to develop a pattern-driven framework, built upon existing IoT platforms, to enable and guarantee secure and dependable actuation and semi-autonomic behavior in IoT/IIoT applications	This framework support cross-layer intelligent dynamic adaptation, including heterogeneous smart objects, networks, and clouds, addressing effective adaptation and autonomic behavior at the field (edge) and infrastructure (backend) layers based on intelligent analysis and learning	https://cordis.europa.eu/project/rcn/213548_en.html
8	SCOTT	This project aims to develop trust in wireless solutions and to improve the social acceptability of IoT at a full pace. In this project, there are 57 key partners from 12 countries, to provide an effective solution for wireless and IoT challenges, like an end to end security, interoperability, and reliable connectivity	Its focus is on WSN and actuator networks. Also, it is working on smart infrastructure health and communication in mobility, thus addressing essential European societal challenges and significantly working on urgent issues like Industry 4.0 and Automated vehicles	https://scottproject.eu/
9	EPoCH	The work aims to prevent specific dangerous attacks like the backdoor attack in the cryptography of IoT devices. It causes a complete system loss of security. Finding the countermeasure of the attack on the cryptographic algorithm is also the goal of this project	This project works on the following two main modules: In the first module, the aim is to actively design the fundamental countermeasure for the attack, which is analogous for the cryptoanalysis. Finding the consequences of system security Secondly, the development of a detection based pro-active approach, that provides systematic protection against illegitimate manipulators	https://www.openaire.eu/search/project?projectId=corda__h2020::acf64d5d0a9b0661540820c3ae523869
10	DOGANA	To reduce the modern social engineering 2.0 vulnerability risk and to deploy efficient methods to fill the gap by designing a framework	This project is doing work on advanced social engineering security model. It is also providing an insurance model for cyber-attack risks	https://www.dogana-project.eu/index.php

Table 6 (continued)

S. nos.	Project name	Aim of research	Area of research	HTTPS location
11	WORLDTIMING II	The aim of this project's second phase is to provide security against Global Navigation Satellite System (GNSS) receivers signal vulnerabilities and guarantee an ultra-accurate time distribution using the existing telecommunication network	The project is working on Industrial IoT and distributed systems. It is based on the satellite signal and emphasizing critical applications like smart grid, telecommunication, and finance	https://sevensols.com/index.php/projects/world-timing/
12	BASTION	This research project is working with various security challenges on a lack of resource-constrained devices. It is also working on new ideas of the business model and novel application, for securing the devices against fraud and alteration	The project's area is to develop more secure IoT devices. The project's concentration is on software as well as hardware security. Firmware security is the primary concern for IoT	https://cordis.europa.eu/project/rcn/193687_en.html

List of abbreviations

See Table 7.

Table 7 List of abbreviations

S. nos.	Abbreviation	Meaning
1	3DES	Triple DES
2	3GPP	3rd Generation Partnership Project
3	AC	Attack Cost
4	AES	Advanced Encryption Standard
5	AI	Attack Impact
6	ANN	Artificial Neural Network
7	API	Application Programming Interface
8	ASP	Attack Success Probability
9	AWGN	Additive White Gaussian Noise
10	BLE	Bluetooth Low Energy
11	BPSK	Binary Phase Shift Keying
12	BS	Base Station
13	CBOR	Concise Binary Object Representation
14	CoAP	Constrained Application Protocol
15	COSE	CBOR Object Encryption and Signing
16	CPS	Cyber-Physical System
17	CWT	CBOR Web Token
18	DARPA	Defense Advanced Research Projects Agency
19	DCM	Device Controller Monitor
20	DDoS	Distributed Denial of Service
21	DES	Data Encryption Standard
22	DESL	DES Lightweight extension
23	DES-X	DES-XOR
24	DSN	Distributed Sensor Network
25	DTLS	Datagram Transport Layer Security
26	DVRs	Digital Video Recorders
27	ECC	Elliptic curve cryptography
28	ED	Eavesdropper Device
29	EEPROM	Electrically Erasable Programmable ROM
30	eMTC	enhanced M/c Type Communication
31	EPC Global	Electronics Product Code Global
32	FPGA	Field Programmable Gate Array
33	GSM	Global System for Mobile communication
34	HLA	Hybrid lightweight algorithm
35	IDS	Intrusion Detection System
36	IETF	Internet Engineering Task Force
37	IoBT	Internet of Battlefield Things
38	IoT	Internet of Things
39	ISO	International Standards Organization

Table 7 (continued)

S. nos.	Abbreviation	Meaning
40	JSON	JavaScript Object Notation
41	JWT	JSON Web Token
42	LISA	Lightweight Security Algorithm for wireless
43	LISP	Lightweight Security Protocol
44	LPWAN	Low Power Wide Area Network
45	LSec	Lightweight Security Protocol
46	LTE	Long Term Evolution
47	M2M	Machine to Machine communication
48	ML	Machine Learning
49	MTTC	Mean-time-to-Compromise
50	NB-IoT	Narrowband-Internet of Things
51	NOMA	Non Orthogonal Multiple Access
52	NTC	Near-Threshold Computing
53	O-TRAP	Optimistic Trivial RFID Authentication Protocol
54	PaaS	Platform as a Services
55	PD	Pulse Generator
56	PROM	Programmable Read-Only Memory
57	PUF	Physically Unclonable Function
58	QPSK	Quadrature Phase Shift Keying
59	REST	Representational State Transfer
60	RFID	Radio Frequency and Identification
61	SaaS	Software as a Service
62	SCADA	Supervisory Control And Data Acquisition
63	SC-FDMA	Single Carrier- Frequency Division Multiple Access
64	SD	Smart Device
65	SINR	Signal Interference Noise Ratio
66	SIOT	Social Internet of Things
67	SITP	Secure Internet of Things Project
68	SMS	Short Messaging Services
69	SNMP	Simple Network Management Protocol
70	SNR	Signal to Noise Ratio
71	SoA	Service-oriented Architecture
72	SOP	Secrecy Outage probability
73	SPINS	Security Protocols in sensor Networks
74	SR	Secrecy Rate
75	TEA	Tiny Encryption Algorithm
76	TLS	Transport Layer Security
77	UDP	User Datagram Protocol
78	UL/DL	Up Link/Down Link
79	Wi-Fi	Wireless Fidelity
80	WLAN	Wireless Local Area Network
81	WoT	Web of Things
82	WSN	Wireless Sensor Network
83	XTEA	Extended TEA

References

1. Granjal, J., Monteiro, E., & SáSilva, J. (2015). Security for the Internet of Things: A survey of existing protocols and open research issues. *IEEE Communications Surveys & Tutorials, 17*(3), 1294–1312.
2. Sajid, A., Abbas, H., & Saleem, K. (2016). Cloud-assisted IoT-based SCADA systems security: A review of the state of the art and future challenges. *IEEE Access, 4,* 1375–1384.
3. Razzaque, M. A., Milojevic-Jevric, M., Palade, A., & Clarke, S. (2016). Middleware for Internet of Things: A Survey. *IEEE Internet of Things Journal, 3*(1), 70–95.
4. Gozalvez, J. (2016). New 3GPP standard for IoT (mobile radio). *IEEE Vehicular Technology Magazine, 11*(1), 14–20.
5. Li, S., Xu, L. D., & Zhao, S. (2014). *The Internet of Things: A survey* (pp. 243–259). New York: Springer.
6. Frustaci, M., Pace, P., Aloi, G., & Fortino, G. (2017). Evaluating critical security issues of the IoT world: Present and future challenges. *IEEE Internet of Things Journal, 5*(4), 2483–2495.
7. Atzori, L., Iera, A., & Morabito, G. (2010). The Internet of Things: A survey. *Computer Networks, 54,* 2787–2805.
8. Miorandi, D., Sicari, S., Pellegrini, F. D., & Chlamtac, I. (2012). Internet of Things: Vision, applications, and research challenges. *Ad Hoc Networks, 10*(7), 1497–1516.
9. Singh, S., Sharma, P. K., Moon, S. Y., & Park, J. H. (2017). Advanced lightweight encryption algorithms for IoT devices: Survey, challenges, and solutions. *Journal of Ambient Intelligence and Humanized Computing*. https://doi.org/10.1007/s12652-017-0494-4.
10. Cheng, C., Lu, R., Petzoldt, A., & Takagi, T. (2017). Securing the Internet of Things in a quantum world. *IEEE Communications Magazine, 55*(2), 116–120.
11. Bormann, C., Castellani, A. P., & Shelby, Z. (2012). CoAP: An application protocol for billions of tiny internet nodes. *IEEE Internet Computing, 1*(2), 62–67.
12. Premnath, S. N., & Haas, Z. J. (2015). Security and privacy in the Internet-of-Things under time-and-budget-limited adversary model. *IEEE Wireless Communications Letters, 4*(3), 277–280.
13. Liu, J., & Sun, W. (2016). Smart attacks against intelligent wearables in people-centric Internet of Things. *IEEE Communications Magazine, 54,* 44–49.
14. Sedjelmaci, H., Senouci, S. M., & Taleb, T. (2017). An accurate security game for low-resource IoT devices. *IEEE Transactions on Vehicular Technology, 66,* 9381–9393.
15. Cheng, S. M., Chen, P. Y., Lin, C. C., & Hsiao, H. C. (2017). Traffic-aware patching for cyber security in mobile IoT. *IEEE Communications Magazine, 55,* 29–35.
16. Chen, J., Hu, K., Wang, Q., Sun, Y., Shi, Z., & He, S. (2017). Narrowband internet of things: Implementations and applications. *IEEE Internet of Things Journal, 4*(6), 2309–2314.
17. Elsaadany, M., Ali, A., & Hamouda, W. (2017). Cellular LTE-A technologies for the future Internet-of-Things: Physical layer features and challenges. *IEEE Communications Surveys & Tutorials, 19*(4), 2544–2572.
18. Yang, W., Wang, M., Zhang, J., Zou, J., Hua, M., Xia, T., et al. (2017). Narrow band wireless access for low-power massive internet of things: A bandwidth perspective. *IEEE Wireless Communications, 24*(3), 138–145.
19. Finnegan, J., & Brown, S. (2018). A comparative survey of LPWA networking.
20. Juels, A. (2006). RFID security and privacy: A research survey. *IEEE Journal on Selected Areas in Communications, 24*(2), 381–394.
21. http://www.radio-electronics.com/info/wireless/radio-frequency-identifi-cation-rfid/iso-epcglobal-iec-standards.php.
22. Bu, K., Xu, M., Liu, X., Luo, J., Zhang, S., & Weng, M. (2015). Deterministic detection of cloning attacks for anonymous RFID systems. *IEEE Transactions on Industrial Informatics, 11*(6), 1255–1266.
23. Xiao, Q., Gibbons, T., & Lebrun, H. (2008). RFID technology, security vulnerabilities, and countermeasures.
24. Burmester, M., & De Medeiros, B. (2007). RFID security: Attacks, countermeasures and challenges. In *The 5th RFID academic convocation, the RFID journal conference*.
25. Rotter, P. (2008). A framework for assessing RFID system security and privacy risks. *IEEE Pervasive Computing, 7*(2), 70–77.
26. Bu, K., Weng, M., Zheng, Y., Xiao, B., & Liu, X. (2017). You can clone but you cannot hide: A survey of clone prevention and detection for RFID. *IEEE Communications Surveys & Tutorials, 19*(3), 1682–1700.
27. Wang, K. H., Chen, C. M., Fang, W., & Wu, T. Y. (2017). On the security of a new ultra-lightweight authentication protocol in IoT environment for RFID tags. *The Journal of Supercomputing, 74,* 65–70.

28. Fan, K., Jiang, W., Li, H., & Yang, Y. (2018). Lightweight RFID protocol for medical privacy protection in IoT. *IEEE Transactions on Industrial Informatics, 14*(4), 1656–1665.
29. https://www.silabs.com/documents/public/white-papers/evolution-of-wir-eless-sensor-networks.pdf.
30. Wang, Q., & Balasingham, I. (2010). Wireless sensor networks—An introduction. In Y. Kheng Tan (Ed.), *Application-centric design*. ISBN: 978-953-307-321-7.
31. Jha R. K., Dalal, U. D. & Bholebawa, I. Z. (2012). Performance analysis of black hole attack on WiMAX-WLAN interface network. In *Third international conference on computer and communication technology*, Allahabad, pp. 303–308.
32. Liu, Y., Dong, M., Ota, K., & Liu, A. (2016). ActiveTrust: Secure and trustable routing in wireless sensor networks. *IEEE Transactions on Information Forensics and Security, 11*(9), 2013–2027.
33. Sen, A., & Madria, S. (2017). Risk assessment in a sensor cloud framework using attack graphs. *IEEE Transactions on Services Computing, 10*(6), 942–955.
34. Yuxing, M., Huiyuan, Z., & Dongmei, Y. (2018). Weak node protection to maximize the lifetime of wireless sensor networks. *Journal of Systems Engineering and Electronics, 29*(4), 693–706.
35. Gandino, F., Ferrero, R., & Rebaudengo, M. (2017). A key distribution scheme for mobile wireless sensor networks: q-s-composite. *IEEE Transactions on Information Forensics and Security, 12*(1), 34–47.
36. Guinard, D., Trifa, V., Mattern, F., & Wilde, E. (2011). From the Internet of Things to the Web of Things: Resource oriented architecture and best practices.
37. Xie, W., Tang, Y., Chen, S., Zhang, Y., & Gao, Y. (2016). *Security of Web of Things: A survey* (pp. 61–70). Dordrecht: Springer.
38. Barka, E., Mathew, S. S., & Atif, Y. (2015). *Securing the Web of Things with role-based access control* (pp. 14–26). Dordrecht: Springer.
39. Jing, Q., Vasilakos, A. V., Wan, J., Lu, J., & Qiu, D. (2014). Security of the Internet of Things: Perspectives and challenges. *Wireless Network, 20,* 2481–2501. https://doi.org/10.1007/s11276-014-0761-7.
40. Bandyopadhyay, D., & Sen, J. (2011). Internet of Things: Applications and challenges in technology and standardization. *Wireless Personal Communication, 58,* 49–69.
41. Xu, L. D., He, W., & Li, S. (2014). Internet of Things in industries: A Survey. *IEEE Transactions on Industrial Informatics, 10*(4), 2233–2243.
42. Ge, M., Hong, J. B., Guttmann, W., & Kim, D. S. (2017). A framework for automating security analysis of the internet of things. *Journal of Network and Computer Applications, 83,* 12–27.
43. Hashizume, K., Rosado, D. G., Fernández-Medina, E., & Fernandez, E. B. (2013). An analysis of security issues for cloud computing. *Journal of internet services and applications., 4*(1), 5.
44. Shah, H., Anandane, S. S., & Shrikanth. (2013). Security issues on cloud computing. arXiv:1308.5996.
45. Aris, A., Oktug, S. F., & Yalcin, S. B. O. (2015). Internet-of-Things security: Denial of service attacks. In *Signal processing and communications applications conference* (SIU).
46. Illiano, V. P., & Lupu, E. C. (2015). Detecting malicious data injections in event detection wireless sensor networks. *IEEE Transactions on Network and Service Management, 12*(3), 496–510.
47. Xu, K., Zhang, X., Song, M., & Song, J. (2009). Mobile Mashup: Architecture, challenges and suggestions. *International Conference on Management and Service Science, Wuhan, 2009,* 1–4.
48. Feng, Y., Wang, W., Weng, Y., & Zhang, H. (2017). A replay-attack resistant authentication scheme for the Internet of Things. In *IEEE international conference on computational science and engineering (CSE) and IEEE international conference on embedded and ubiquitous computing (EUC)*, Guangzhou, pp. 541–547.
49. Cyr, B., Horn, W., Miao, D., Specter, M. (2014). Security analysis of wearable fitness devices (Fitbit). Massachusetts Institute of Technology Cambridge, Massachusetts, USA.
50. Cekerevac, Z., Dvorak, Z., Prigoda, L., & Cekerevac, P. (2017). Internet of Things and the man-in-the-middle attacks-security and economic risks. *MEST Journal, 5*(2), 15–25.
51. Mohammadi, S., & Jadidoleslamy, H. (2011). A comparison of link layer attacks on wireless sensor networks. *International Journal on Applications of Graph Theory in Wireless Ad Hoc Networks and Sensor Networks (GRAPH-HOC), 3*(1), 35–56.
52. Zhang, K., Liang, X., Lu, R., & Shen, X. (2014). Sybil attacks and their defenses in the Internet of Things. *IEEE Internet of Things Journal, 1*(5), 372–383.
53. Campus, N. M., Govindapura, G., & Yelahanka, B. (2018). Denial-of-service or flooding attack in IoT routing. *International Journal of Pure and Applied Mathematics., 118*(19), 29–42.
54. Benzarti, S., Triki, B., & Korbaa, O. (2018). Survey on attacks in Internet of Things based networks. In *2017 International conference on engineering & MIS (ICEMIS)*.
55. Mosenia, A., & Jha, N. K. (2016). A comprehensive study of security of internet-of-things. *IEEE Transactions on Emerging Topics in Computing., 5*(4), 586–602.

56. Salehi, A., Razzaque, M. A., Naraei, P., & Farrokhtala, A. (2013). Detection of sinkhole attack in wireless sensor networks. In *IEEE international conference on space science and communication (IconSpace)*, pp. 361–365.
57. Namvar, N., Saad, W., Bahadori, N., & Kelley, B. (2016). Jamming in the Internet of Things: A game-theoretic perspective. In *IEEE global communications conference (GLOBECOM)*, pp. 1–6.
58. Jokhio, S. H., Jokhio, I. A., & Kemp, A. H. (2012). Node capture attack detection and defence in wireless sensor networks. *IET Wireless Sensor Systems, 2*(3), 161–169.
59. Abawajy, J. (2009). Enhancing RFID tag resistance against cloning attack. In *2009 Third international conference on network and system security*, Gold Coast, QLD, pp. 18–23.
60. Ling, Z., Luo, J., Xu, Y., Gao, C., Wu, K., & Fu, X. (2017). Security vulnerabilities of Internet of Things: A case study of the smart plug system. *IEEE Internet of Things Journal, 4*(6), 1899–1909.
61. Singh, S., Sharma, P. K., Moon, S. Y., & Park, J. H. (2017). *Advanced lightweight encryption algorithms for IoT devices: Survey, challenges, and solutions*. Berlin: Springer.
62. Yang, X., Wang, X., Wu, Y., Qian, L. P., Lu, W., & Zhou, H. (2018). Small-cell assisted secure traffic offloading for narrowband Internet of Thing (NB-IoT) systems. *IEEE Internet of Things Journal, 5*(3), 1516–1526.
63. Safi, A. (2017). Improving the security of Internet of things using encryption algorithms. *World Academy of Science, Engineering and Technology, International Journal of Computer and Information Engineering, 11*(5), 546–549.
64. Lee, J., & Lim, D. (2014). Parallel architecture for high-speed block cipher, HIGHT. *International Journal of Security and Its Applications, 8*(2), 59–66.
65. Shen, S., Huang, L., Zhou, H., Yu, S., Fan, E., & Cao, Q. (2018). Multistage signaling game-based optimal detection strategies for suppressing malware diffusion in fog-cloud-based IoT networks. *IEEE Internet of Things Journal, 5*(2), 1043–1054.
66. Usman, M., Ahmed, I., Aslam, M. I., Khan, S., & Shah, U. A. (2017). SIT: A lightweight encryption algorithm for secure Internet of Things. *International Journal of Advanced Computer Science and Applications, 8*(1), 2017. https://doi.org/10.14569/IJACSA.2017.080151.
67. Xiao, G., Guo, J., Xu, L. D., & Gong, Z. (2014). User interoperability with heterogeneous IoT devices through transformation. *IEEE Transactions on Industrial Informatics, 10*(2), 1486–1496.
68. Kar, S. (2014). Internet of Things will multiply the digital universe data to 44 trillion GBs by 2020 (online document). http://cloudtimes.org/2014/04/17/internet-of-things-will-multiply-thedigital-universe-data-to-44-trillion-gbs-by-2020.
69. Bandyopadhyay, D., & Sen, J. (2011). Internet of Things: Applications and challenges in technology and standardization. *Wireless Personal Communications, 58*(1), 49–69.
70. Islam, S. M. R., Kwak, D., Kabir, M. H., Hossain, M., & Kwak, K. S. (2015). The Internet of Things for health care: A comprehensive survey. *IEEE Access, 3,* 678–708.
71. Boisguene, R., Tseng, S. C., Huang, C. W., & Lin, P. (2017). A survey on NB-IoT downlink scheduling: issues and potential solutions. In *International wireless communications and mobile computing conference,* pp. 547–551.
72. Hoymann, C., Astely, D., Stattin, M., Wikström, G., Cheng, J. F., Höglund, A., et al. (2016). LTE release 14 outlook. *IEEE Communication Magazine, 54,* 44–49.
73. Rico-Alvarino, A., et al. (2016). An overview of 3GPP enhancements on machine to machine communications. *IEEE Communications Magazine, 54*(6), 14–21.
74. Rajashree, S., Soman, K. S., & Shah, P. G. (2018). Security with IP address assignment and spoofing for smart IOT devices. In *2018 international conference on advances in computing, communications and informatics (ICACCI)*, Bangalore, pp. 1914–1918.
75. Gupta, A., Jha, R. K., Gandotra, P., & Jain, S. (2018). Bandwidth spoofing and intrusion detection system for multistage 5G wireless communication network. *IEEE Transactions on Vehicular Technology, 67*(1), 618–632.
76. Barros, J., & Rodrigues, M. R. D. (2006). Secrecy capacity of wireless channels. In *2006 IEEE international symposium on information theory*, Seattle, WA, pp. 356–360.
77. Rawat, D. B., White, T., Parwez, M. S., Bajracharya, C., & Song, M. (2017). Evaluating secrecy outage of physical layer security in large-scale MIMO wireless communications for cyber-physical systems. *IEEE Internet of Things Journal, 4*(6), 1987–1993.
78. Zou, Y., Zhu, J., Wang, G., & Shao, H. (2014). Secrecy outage probability analysis of multi-user multi-eavesdropper wireless systems. In *2014 IEEE/CIC international conference on communications in China (ICCC)*, Shanghai, pp. 309–313.
79. Chen, G., Coon, J. P., & Di Renzo, M. (2017). Secrecy outage analysis for downlink transmissions in the presence of randomly located eavesdroppers. *IEEE Transactions on Information Forensics and Security, 12*(5), 1195–1206.

80. Chrysikos, T., Dagiuklas, T., & Kotsopoulos, S. (2010). A closed-form expression for outage secrecy capacity in wireless information: Theoretic security. Wireless Telecommunications Laboratory, pp. 3–12.
81. PACEMAKER System Specification. (2007). Copyright 2007 Boston Scientific January 3.
82. Brachmann, M., Keoh, S. L., Morchon, O. G., & Kumar, S. S. (2012). End-to-end transport security in the IP-based Internet of Things. In *2012 21st International conference on computer communications and networks (ICCCN)*, Munich, pp. 1–5.
83. Rullo, A., Midi, D., Serra, E., & Bertino, E. (2017). Pareto optimal security resource allocation for Internet of Things. *ACM Transactions on Privacy and Security, 20*(4), 1–30.
84. Wu, H., & Wang, W. (2018). A game theory based collaborative security detection method for Internet of Things systems. *IEEE Transactions on Information Forensics and Security, 13*(6), 1432–1445.
85. Meidan, Y., Bohadana, M., Shabtai, A., Ochoa, M., Tippenhauer, N. O., Guarnizo, J. D., & Elovici, Y. (2017). Detection of unauthorized IoT devices using machine learning techniques. arXiv:1709.04647 v1.
86. Chatterjee, B., Das, D., Maity, S., & Sen, S. (2019). RF-PUF: Enhancing IoT security through authentication of wireless nodes using in-situ machine learning. *IEEE Internet of Things Journal, 6*(1), 388–398.
87. Azmoodeh, A., Dehghantanha, A., & Choo, K. R. (2019). Robust Malware detection for internet of (battlefield) Things devices using deep eigenspace learning. *IEEE Transactions on Sustainable Computing, 4*(1), 88–95.
88. https://ec.europa.eu/programmes/horizon2020/what-horizon-2020.

Mr. Vinod Kumar (S'17) received his B.Tech. in Computer Science and Engineering from Uttar Pradesh Technical University, Lucknow, India, and M.Tech. degree in Computer Science and Engineering from Dr. B.R. Ambedkar National Institute of Technology, Jalandhar, India. He is currently pursuing the Ph.D. degree in Computer Science and Engineering at Shri Mata Vaishno Devi University, Katra, Jammu and Kashmir, India. His Research Interest includes emerging technology, like Internet of Things. He is currently working on security issues on Narrowband- Internet of Things. His area of interest is Network Security, Cryptography, and Computer network. He is working on MATLAB, SystemVue, and Python for his research work. He has received the teaching assistantship from 2006–2008 and since 2017 through MHRD. He is a student member of IEEE.

Dr. Rakesh K Jha (S'10, M'13, SM'15) is currently an Associate Professor in the School of Electronics and Communication Engineering, Shri Mata Vaishno Devi University, Katra, Jammu and Kashmir, India. He is carrying out his research in wireless communication, power optimizations, wireless security issues, and optical communications. He has done B.Tech. in Electronics and Communication Engineering from Bhopal, India, and M. Tech from NIT Jalandhar, India. He has received his Ph.D. degree from NIT, Surat, India, in 2013. He has published more than 45 Science Citation Index Journals Papers Including many IEEE Transactions, IEEE Journal, and more than 25 International Conference papers. His area of interest is Wireless communication, Optical Fiber Communication, Computer Networks, and Security issues. Dr. Jha's one concept related to the router of Wireless Communication was accepted by ITU (International Telecommunication Union) in 2010. He has received the young scientist author award by ITU in Dec 2010. He has received APAN fellowship in 2011, 2012,

2017, and 2018 and a student travel grant from COMSNET 2012. He is a senior member of IEEE, GISFI and SIAM, International Association of Engineers (IAENG), and ACCS (Advanced Computing and Communication Society). He is also a member of ACM and CSI, many patents, and more than 2161 citations in his credit.

Prof. Sanjeev Jain (M'16) born at Vidisha in Madhya Pradesh in 1967, obtained his Post Graduate Degree in Computer Science and Engineering from the Indian Institute of Technology, Delhi, in 1992. He later received his Doctorate Degree in Computer Science and Engineering and has over 24 years' experience in teaching and research. He has served as Director, Madhav Institute of Technology and Science (MITS), Gwalior. He has also served as vice-chancellor of Shri Mata Vaishno Devi University, Katra, Jammu and Kashmir, India. Presently, he is working as a Director at Indian Institute of Information Technology Design and Manufacturing, Jabalpur. Besides teaching at Post Graduate level, Professor Jain has the credit for making a significant contribution to R&D in the area of Image Processing and Mobile Adhoc Network. He has guided Ph.D. Scholars and has undertaken a number of significant R&D projects sponsored by the Government and Private Agencies. His work on Digital Watermarking for Image Authentication is highly valued in the research field.

Terms and Conditions

Springer Nature journal content, brought to you courtesy of Springer Nature Customer Service Center GmbH ("Springer Nature").

Springer Nature supports a reasonable amount of sharing of research papers by authors, subscribers and authorised users ("Users"), for small-scale personal, non-commercial use provided that all copyright, trade and service marks and other proprietary notices are maintained. By accessing, sharing, receiving or otherwise using the Springer Nature journal content you agree to these terms of use ("Terms"). For these purposes, Springer Nature considers academic use (by researchers and students) to be non-commercial.

These Terms are supplementary and will apply in addition to any applicable website terms and conditions, a relevant site licence or a personal subscription. These Terms will prevail over any conflict or ambiguity with regards to the relevant terms, a site licence or a personal subscription (to the extent of the conflict or ambiguity only). For Creative Commons-licensed articles, the terms of the Creative Commons license used will apply.

We collect and use personal data to provide access to the Springer Nature journal content. We may also use these personal data internally within ResearchGate and Springer Nature and as agreed share it, in an anonymised way, for purposes of tracking, analysis and reporting. We will not otherwise disclose your personal data outside the ResearchGate or the Springer Nature group of companies unless we have your permission as detailed in the Privacy Policy.

While Users may use the Springer Nature journal content for small scale, personal non-commercial use, it is important to note that Users may not:

1. use such content for the purpose of providing other users with access on a regular or large scale basis or as a means to circumvent access control;
2. use such content where to do so would be considered a criminal or statutory offence in any jurisdiction, or gives rise to civil liability, or is otherwise unlawful;
3. falsely or misleadingly imply or suggest endorsement, approval , sponsorship, or association unless explicitly agreed to by Springer Nature in writing;
4. use bots or other automated methods to access the content or redirect messages
5. override any security feature or exclusionary protocol; or
6. share the content in order to create substitute for Springer Nature products or services or a systematic database of Springer Nature journal content.

In line with the restriction against commercial use, Springer Nature does not permit the creation of a product or service that creates revenue, royalties, rent or income from our content or its inclusion as part of a paid for service or for other commercial gain. Springer Nature journal content cannot be used for inter-library loans and librarians may not upload Springer Nature journal content on a large scale into their, or any other, institutional repository.

These terms of use are reviewed regularly and may be amended at any time. Springer Nature is not obligated to publish any information or content on this website and may remove it or features or functionality at our sole discretion, at any time with or without notice. Springer Nature may revoke this licence to you at any time and remove access to any copies of the Springer Nature journal content which have been saved.

To the fullest extent permitted by law, Springer Nature makes no warranties, representations or guarantees to Users, either express or implied with respect to the Springer nature journal content and all parties disclaim and waive any implied warranties or warranties imposed by law, including merchantability or fitness for any particular purpose.

Please note that these rights do not automatically extend to content, data or other material published by Springer Nature that may be licensed from third parties.

If you would like to use or distribute our Springer Nature journal content to a wider audience or on a regular basis or in any other manner not expressly permitted by these Terms, please contact Springer Nature at

onlineservice@springernature.com