Computer Networks 185 (2021) 107592

Contents lists available at ScienceDirect

Computer Networks

journal homepage: www.elsevier.com/locate/comnet

Layer based security in Narrow Band Internet of Things (NB-IoT)

Rakesh Kumar Jha [a,*], Puja [b], Haneet Kour [a], Manoj Kumar [b], Shubha Jain [c]

[a] School of Electronics and Communication Engineering, Shri Mata Vaishno Devi University, Jammu and Kashmir, India
[b] School of Computer Science and Engineering, Shri Mata Vaishno Devi University, Jammu and Kashmir, India
[c] Telecommunications from the University of Maryland, College Park, USA

ARTICLE INFO

Keywords:
IoT
Bug
Security
MEMS
Secrecy rate (SR)
Secrecy outage probability (SOP)

ABSTRACT

In the recent years, the growth of technology and the resulting transformation is happening at a rapid pace. In this junction, IoT has provided a great platform and bridge between these technologies. A lot of research regarding the application of IoT Systems has been done in the recent years but one area that lacks research is security issues in Narrow Band Internet of Things (NB-IoT).It is noticed that security and Privacy in NB-IoT system is a challenging task for researchers and academia. Application of NB-IoT in Defense security opened a new way for the researchers but at the same time security threat can lead to drastic loss. Nowadays, MEMS-NB-IoT device (Bug)/ BOT are being used for carrying out any malicious security attack. This can be a serious area of concern in the case of defense security. These MEMS device are very dangerous and it can spoof data from any type of network. The size of this device is very small, it can travel to any location for monitoring the enemy movement, and it is very difficult to identify these types of bugs. These BOT device very sensitive at Perception and Network Layered. In this paper, we have provided detail analysis of IoT/NB-IoT Layered architecture. A novel proposal depicting security attack in a Smart home system with IoT and NB-IoT enabled devices is presented. The Secrecy Rate (SR), the Secrecy Outage Probability (SOP) is being calculated, and performance analysis of IoT system in the presence of Bugs for a smart home system is carried out. Simulations have been performed and the performance analysis done is based on Security non-outage probability vs security rate with real time analysis.

1. Introduction

Green Internet of things shortly termed, as IoT is one of the eminent technologies in the coming future. The term IOT had its origin in 1999, when Kevin Ashton during his work at Procter and Gamble coined the term for the promotion of RFID technology in his presentation. After that for about 10 years, it did not get any consideration. However, in 2014, the IoT technology got mass marked attention.

It was expected that this technology would make the life of human being smarter and much easier. The world of IoT is expected to be completely different from the today's world. Using IoT, A person can control anything from anywhere according to his convenience. This will save money as well as time. This technology is far- ranging technology that has its application in each field. Internet is the backbone of IoT Systems. It is the fusion of multiple technologies like real time analysis, sensor networks, machine learning etc. All these technologies converge together to enable the Internet of Things. The IoT systems generally include a number of computing devices that are interconnected with each other. These computing devices include Digital Machines, Mechanical Machines, any physical object embedded with sensors or microcontroller chips connected to the internet. These devices have ability to transfer data over the network and controlled remotely.

IoT is related to Machine-to-Machine Communication (M2M). In M2M, two machines communicate with each other through a network and there is no human intervention. Similarly, IoT devices connect with each other through a network and human intervention is required only for setting up and during repair. Nowadays, IoT has its application in the real world which includes Smart homes (controlling and accessing home appliances, lighting, electronic devices remotely), Smart Appliances, wearable smart devices, Smart City, Smart Grid Smart health care facilities (for observing patients more closely like heart chip implant), Smart farming (sensing light, temperature, humidity, moisture content of the soil in a crop field) and many more. IoT is being used by many organizations for working more efficiently. It is an advance technology

* Corresponding author.
E-mail addresses: jharakesh.45@gmail.com (R.K. Jha), pujajhasmvdu@gmail.com (Puja), hani.kpds@gmail.com (H. Kour), vermamk@gmail.com (M. Kumar), shubhajain1203@gmail.com (S. Jain).

https://doi.org/10.1016/j.comnet.2020.107592
Received 11 November 2019; Received in revised form 27 August 2020; Accepted 6 October 2020
Available online 9 October 2020

and can save money and time consecutively. Another important area of concern is the security and privacy of devices that are linked with Internet of Things. IoT has got a great criticism related to its privacy and security.

1.1. Background

Various IoT system are divided into different layers: Perception Layer, Network Layer, Service management Layer, Application layer, and Business layer. Each layer has its own functionality [1]. These layers work together to form a complete IoT system. Data collected at the Perception layer is analyzed at the business layer and the intermediate layers help in transferring the data efficiently and securely. Fig. 1 shows the layered architecture of IoT.

Characteristics and functionality of each layer is discussed as following:

1. Perception Layer:

This layer deals with the collection of data from the physical events and the conditions. This collection of data is done with the help of Sensors and actuators that sense the changes in the conditions and make measurements. Sensors at the perception layer generate electronic signals triggered from physical event /condition. These electronic signals are aggregated at gateways. This layer is generally concerned with the collection of data and processing with the help of various technologies like Global Positioning System (GPS), Wireless Sensor Network (WSN), Radio- Frequency Identification (RFID) and RFID Sensor Network (RSN). After the collection of data, it is transferred to Network layer through Gateway. This layer is most sensitive for Physical Layer attacks like jamming, scrambling etc. Intruder is mostly targeted on this layer to spoof the data.

2. Network Layer:

This layer is related to providing access to the access network. The data collected from the perception layer is transmitted to the particular system for processing through this layer. This layer makes use of modern access technologies and protocols like IPV6/IPV4/LoWPAN. With the help of this layer, things can be connected with other things, which is the main aspect of IoT system for managing the event intelligently. From the network layer the data is then transferred to the Service Management layer. After Physical Layer this layer is sensitive towards security attacks, at this layer intruder spoof the NBIoT/IoT networks using attacks like DoS, DDoS, Bandwidth spoofing, IP Spoofing etc.

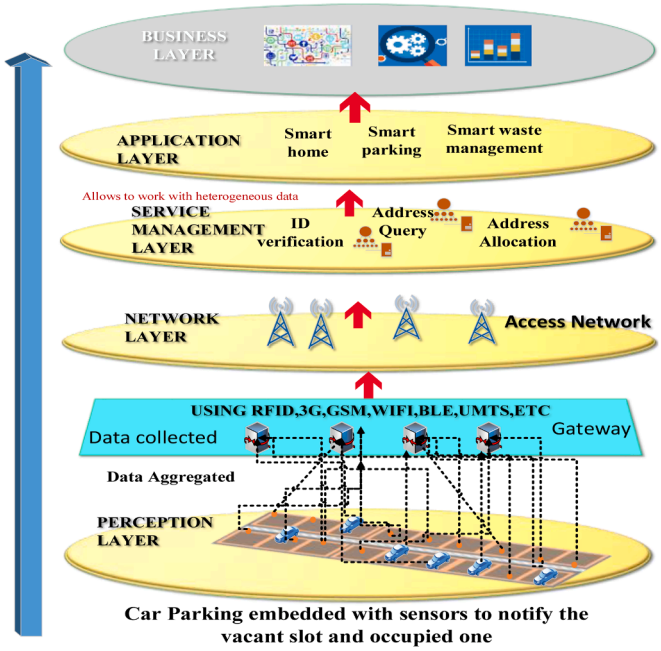

Fig. 1. Layered architecture of IoT.

3. Service Management Layer:

Service management layer is the main layer that opens up the services and applications of IoT. It depends on the middleware technology that presents an efficient platform. This layer provides services by pairing based on addresses and it process the data received. Various activities like exchange of information and management of data is performed at the Service Management Layer.

4. Application Layer:

Application layer comprises of applicable part of whole system, which is concerned to provide the service demanded by specific user. This layer makes use of various protocols that generally includes MQTT (Message Queue Telemetry Transport), CoAP (Constrained Application Protocol). These protocols helps in providing the requested service to the user efficiently.

5. Business Layer:

Business Layer is the final most layer and at this layer, data analysis is done based on data received from the application layer. At this layer, it is very important that privacy of the user be maintained. With this layer, the whole IoT system preforms like an intelligent system, where the machines are interconnected with the help of internet and less intervention of human is required.

1.2. Related work

Exhaustive surveys are available in the literature that study NB-IoT and related aspects due to increased popularity of Low Power Wireless Access (LWPA) devices The authors in [2] review in detail the technology, its architectural aspects, combination with latest cellular technologies and also discuss some open issues in NB-IoT. The operation of NB-IoT from the perspective of cloud-RAN implementation is also discussed in [3]. The security aspects relating to NB-IoT are presented in [4] wherein the authors propose an algorithm for optimizing the pairing between a smart device and access point to improve the security and throughput obtained. Another survey in [5] discusses the issues in NB-IoT downlink scheduling to efficiently use the limited spectrum available and suggests some potential solutions.

There are various surveys and works that study security and privacy aspects including the different attacks at individual layers in an IoT architecture. The authors in [6] present a detailed survey on NB-IoT security studying technologies such as RFID, WSN, WOT etc. Another survey on IoT security by authors of [7] depicts the challenges in IoT security with some potential architectures incorporating technologies such as block chain, machine learning and so on to elevate the security levels. Various trust management techniques for IoT are surveyed in [8] along with their pros and cons. Certain works in literature discuss the security issues pertaining to different architectural layers such as node capturing attacks [9], eavesdropping and interference [10] at the sensing layer. Security attacks at the network layer include phishing site attack [11], access attack [12], DDOS/DOS attack [13] among various others.

The service management layer or the middleware layer between the network layer and the application layer has security threats such as SQL Injection attack [14], signature-wrapping attack [15]. Application layer is the layer that directly deals with the end users. Application such as

Smart Home, Smart Cities fall in this layer. The major security issues relating to this layer are of data theft and privacy. Some other major threats are sniffing attack [16] used to monitor the data traffic in IoT applicaton and have an access to the confidential data. Another attack called Reprogram attack [17] can interfere with the programming process of the application and hijack the IoT network.

1.3. Contributions and organization

This article presents a detailed analysis of security and privacy aspects in NB-IoT enabled devices and related application areas. The major contributions are as follows:

- The security and privacy aspects in NB-IoT are analyzed in every layer according to the functionality of each layer.
- The application areas that are real time threats on the IoT system are discussed.
- An architecture is proposed for a Smart Home system studying a real time scenario to analyze the security issues in NB-IoT using MEMS IoT device.
- The performance analysis of the proposal is done to study the secrecy rate in presence and absence of a bug/BOT.

The rest of the paper is organized as follows. Section II presents the security barriers in NB-IoT discussing the main threats at different layers in an IoT architecture. Section III presents the application areas of IoT security where security and privacy of data is extremely important. A proposed architecture for security issues in NB-IoT with MEMS IoT device is given in Section IV. The performance analysis is given in Section V discussing secrecy rate and secrecy outage probability. The article concludes in Section VI.

2. Security barriers in NB-IoT

Security has always been a very important aspect of human living. In the modern world where science is enduring our life with its inventions safety of our homes, offices and private places is always a need of present human beings. Alarms and event detection will help users to be readily informed about any intrusion detected at home. This system will not only offer intelligent protection from intrusion but will also offer intelligence at the time of any detected event that can lead to a fire outbreak like in case of sudden increase in home temperature or smoke. Alarms and event detectors will make use of sensors placed devices in ideal locations in homes that can constantly communicates with the Narrow Band Internet of Things (NBIoT) network. For the usage of these sensor-enabled devices that can communicate, it is required that they use low data throughput and have good battery life.

Without doubt, NB-IoT is going to provide the next generation with a seamless connectivity and smart services but its service implementation still has a long way to go. There are various key issues related to NB-IoT and one of them is Security of IoT devices and the Privacy of NB-IoT users that are connected to it . In current scenario, researchers are only dealing with energy efficient network deployment for NBIoT network and it is imposing a bigger threat to the use of IoT. Table 1 shows various security barriers and threats concerned with the different layers of IoT/NB-IoT systems that need to be solved. In the table below, the possible threats at each level is presented in a tabulated form [18–35]. For instance at Perception Layer, impersonation attack and the physical attack is very common. At the transportation Layer, Routing attack and Data Transit attack mainly affects the system.

At Application Layer, malicious code injection and data leakage is very common. Each of these attacks is discussed in the later sections of the article.

The layer wise IoT/NB-IoT security attacks are presented in Table 2 along with their counter measures that can be incorporated as possible solutions to prevent these attacks. The brief description of attacks at each layer is given as follows:

Table 1
Threats in IoT/NB-IoT system model [18].

Layer	Main Threats
Application Level	Data Leakage
	DOS Attacks
	Malicious Code Injection
Transportation Level	Routing Attacks
	DoS Attacks
	Data Transit Attacks
Perception Level	Physical Attacks
	Impersonation
	DoS Attacks
	Routing Attacks (e.g. in WSN,RSN)
	Data Transit Attacks (in WSN or RSN)

2.1. Attacks at perception layer

- Physical Attacks: These attacks are mostly performed on the hardware components of NB-IoT systems. The intruder comes close to the system or into the system for carrying out these types of attack. The attacks include tampering of nodes by damaging the nodes or the components of the system. There is requirement of tamper resistant packaging and hiding of nodes to avoid these type of physical attacks on the IoT network.
- Impersonation: In this attack, an intruder makes use of fake identity for getting all the information about the system.
- Jamming Attack: Radio jamming attack occurs at this layer denying services to a valid user. It can be removed by detecting the jammed regions.
- Routing Attacks: The intruder in this type of attack changes the routing table and misleads the data transferred.
- Data Transit Attack: This type of attack usually occurs on the data that is being transferred over the system.
- Eavesdropping Attack: In this attack an eavesdropper intercepts the data being transmitted from the base station to an IoT node and uses it for attacks in future. It can be avoided by isolating the IoT node or using cryptographic algorithms to avoid such attacks.

2.2. Attacks at network layer

- Replay Attack: In this attack, the sensor's resource is consumed by retransmission of a message repeatedly. This attack can be avoided by introducing timestamp and incorporating secure session key management.
- Flooding Attack: In this attack, there is flooding of packets done by an attacker to cause failure in the network. To avoid this attack, a timer limit can be put at the receiver so that if the time limit exceeds the sender can be regarded as an attacker.
- Black hole Attack: In this attack, the attacker depicts that it carries the shortest route to the destination and attracts all the traffic towards itself. This attack can be avoided by detecting the false route and denying any access to the attacker.
- Wormhole attack: In this type of attack, the data packet is displaced from its original location and placed at a distant location. Wormhole detection techniques are required to avoid such attacks in the IoT network.

2.3. Attacks at service management layer

- Service Hijacking: This attack occurs in the lower layers where service provider is responsible for security An application built by the developer is compromised on security due to service provider layer such as PaaS in IoT.

- Third-Party relationship: This attack occurs when more number of data sources are involved and third party services are provided by PaaS. Encryption of the source data is required to avoid such attacks.
- Virtualization threat: In this attack, a virtual machine runs different applications due to which there is extra security required of the virtual layer by using HyperSafe approach.

2.4. Attacks at application layer

- Data leakage: During this attack the NB-IoT devices compromises the privacy of data and results in the leakage of data like private data that generally includes passwords and important user data.
- DoS/DDoS attack: At this layer, the attacker denies the service or application availability to the user by sending large number of requests. There is requirement of high authentication to avoid such attacks.
- Malicious Code Injection: This attack includes the injection of malicious code into the software application and affects the services provided by the system.

2.5. Attacks at business layer

- Data Aggregation Distortion: This attack occurs when the aggregated data is being sent to the base station by the last layer. This data can be distorted by the eavesdropper before it reaches the destination. Protection mechanisms are required to protect the data integrity.

Researchers and academia performed the layer based proposal as per details mentioned in Table 2. The Table briefs the layerwise attacks in an IoT architecture according to the studies from the available literature. The security attacks are discussed with respect to specific application areas such as UAV, Smart Agriculture, Smart Home, Smart Plug system and so on. Based on a particular application in an IoT device the attacks on different layers in an IoT system are highlighted in the Table. The countermeasures or the potential solutions have also been given to ensure security and prevent data theft for IoT device systems. The following section discusses the application areas where security and privacy of data is required to be maintained.

3. Why security of NB-IoT required

These days internet service provides big platform for all types of users. Anyone can contact with anybody at anytime and anywhere. Most of the users are using smart phone or android enabled devices. These devices are enabled with different applications and most of the users are not aware about terms and conditions. Modern Applications requires all type of permissions as if they can access your contacts, pictures, videos, gallery etc. for its better functionalities. However, it can be the source of any privacy attack to our personal data. Nowadays, smart devices like IP-cameras and other sensitive devices that are connected with Wireless LAN (WLAN) i.e. Wi-Fi hotspot are vulnerable to any type of attack. We are also not aware that Wi-Fi hotspots can be hacked by professional intruders that can easily capture any information that is being transferred over the wireless network. These attacks are very sensitive attacks because it is directly related to the personal life of the users. Fig. 2 shows some real time threats and the incidents that is considered as the biggest security attacks on the IoT system [19].

3.1. IoT application areas

IoT is providing great opportunities in all areas like Smart Agriculture, Smart Home, Smart Health, Wearable Devices, Smart appliances and many more.

One of the most important applications of IoT is to provide great opportunity for Smart Industry i.e. Industry Evolution 4.0. By 2022, almost everywhere the services provided will be IoT enabled services.

Fig. 2. Real time threats and incidents on the IoT system.

IoT has found its application in each field of life. Some of its prominent application areas are in the case of Defense and Making homes smarter. Various Characteristics of IoT enabled devices For Defense Purposes and Smart homes is briefly discussed in the following sub sections.

3.2. For defense purposes

Internet of things can be used for defense purposes effectively. It can make the life of soldiers very easy and manageable [25]. Surveying the battlefield and updating officers about the information, they can help them make good decisions at the right time. Fitting of sensors on the military vehicles can help in monitoring the performance and efficiency of the engines so the staff can take that necessary step at correct time. Malfunctioning of any vehicle or machine at the battlefield can lead to heavy loss. Regular checking of these machines and vehicles by the sensor and reporting staff about any fluctuations can be beneficial. Sensors can be attached to the clothes or wearables of the soldiers that could sense their health and alert them for their medical conditions. Internet of Things can be used for remote training for the supervision of their performance, when the data about the soldiers is sent to the couches in the form of video and statistics to supervise them from distance. Fleet and Inventory management on real time basis can be done by making the use of IoT systems.

3.3. For smart home systems

These systems are meant to make the house of present man as a smart system that comprises Smart home devices that can interact with the internet. It consist of three main components: Home Server, Home Gateway and Smart Home Devices [26]. Smart home devices are provided with all the functions that make them suitable for making connection with the internet and can exchange information. These devices are the basic home devices that are being used in day today life like Smart phones, Smart electronic appliances. These smart devices are fitted with sensors and actuators that can communicate with internet and provide information exchange functionalities. The information is transferred with the help of Home Gateway to the Home Server. The Home server provides storage and functions for the integration and distribution of all the information collected from different mediums in the home.

3.4. Unmanned Aerial Vehicle (UAV)

Unmanned Aerial Vehicles are the small air borne vehicles like the aircraft without any human pilot. The Controller that are generally ground based controls these vehicles. UAVs are employed in the areas, which are inaccessible, by the human beings. These vehicles are programmed according to their functions. UAVs used for various purposes like Military border surveillance, carrying aid to the inaccessible areas.

Surveillance of Far-flung areas affected with earthquake or Floods, for increasing the coverage area by acting as the relay or sometimes as the base stations. Thus, UAV are being used for many civil applications [27] because of its easy deployment and low maintenance cost. At some places, multiple UAV's can be used for successful completion of the missions. For multiple UAV communication, networking is enabled to carry out the operation for which they are employed. While setting up of links between the devices, it is always focused that the links that are formed should be reliable and have connectivity in all directions as well as the link performance must be high. For this to be achievable, it is necessary that an efficient wireless technology is required to be implemented. Multiple UAV's behaves like a Flying Adhoc Network (FANET), which is very much similar to the Mobile Adhoc Network (MANET) and Vehicular Adhoc Network (VANET). The FANET is somehow different from MANET and VANET as the network is comprised of flying objects and need more flexible communication techniques so that network can work more effectively.

UAV can be classified based on the operation they are performing [28]. UAV can be Unmanned Ground Vehicle, Unmanned Aerial Vehicle, Unmanned Surface vehicle, Unmanned under water vehicle, Unmanned Spaces craft. By another classification of UAV devices, these vehicles can be classified as the guided and autonomous. Guided vehicles are being controlled whereas the autonomous are fully automatic and are not guided by anyone; they are preprogrammed for the functions they are made for. Based on the Operation Platform the UAV is using they are classified as Low altitude Platform (LAP) and High altitude platform (HAP). Low Altitude Platform can cover altitude less than 10 Km, these LAP UAV are further classified as Vehicle Takeoff and Landing Vehicle (VTOL), Balloons and Aircrafts.

High Altitude Platform UAV can operate up to the altitude above 10kms and are able to stay there for long time. They can move above in the upper layer of atmosphere that is the stratosphere. This HAP UAV are further classified as Airships, Aircrafts and Balloons. This classification is represented in Fig. 3. The next section presents a proposed architecture highlighting the security issues considering a real time Smart Home scenario suing MEMS IoT device.

4. Proposed architecture of security issues in NB-IoT

This section describes the proposed architecture and details of spoofing attacks on system model using IoT MEMS device proposed architecture and system model. In this architecture, BOT device can spoof the bandwidth, Assigned IP associated with valid channels [29,30]. As studied in the previous sections, it is concluded that NB-IoT is not easy to be implemented unless and until the issues related to its implementation will be fulfilled. It is also predictable from the literature survey that IoT is going to be used in every field. Security and Privacy is one of the key issue that needs to get solved. In this section, an architecture for possible security attack in NB-IoT system is presented that is being used in Military applications, Smart Home and Smart Cities. For these applications RFID sensors, IP Cameras, WSN's, RSN are being used for capturing the information. Survey for the Security of RFID is demonstrated in [31,32]. Data from these sensors are then transferred to the IoT Cloud for carrying out the specified IoT application through wireless or wired network. During transferring, the data should be encrypted so that any intruder cannot get the information that is being sent on the network. Besides confidentiality of data there are many other security issues that are already being discussed in the previous sections.

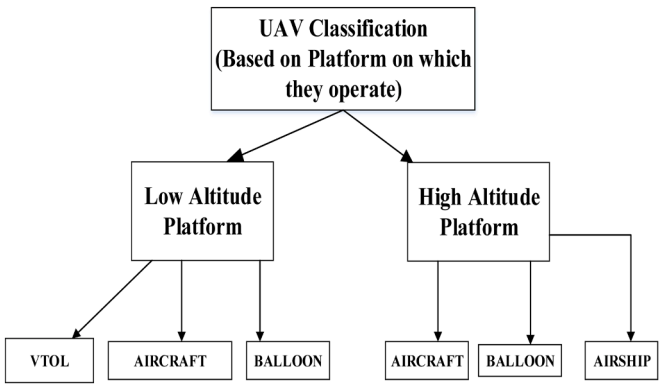

Fig. 3. Classification of UAV based on platform on which it operates.

In the proposed architecture, the attack on NB-IoT system is performed using the UAV MEMS devices. UAV or Drones when invented are like small toys, these were used for delivering of things, for entertaining the children, for monitoring, for capturing videos and photos. But with the development, its capabilities have been improved like improvement in its flying capacity, increasing its stability in air, and many more. Nowadays, UAV is not only being used for entertaining or delivering something, but it is now being used for carrying out special missions where the accessibility is not possible. With the implementation of high-performance micro-electro-mechanical system (MEMS) sensors in UAV, the capabilities of UAV has taken a boon [33,34]. MEMS sensors in combination with the defined software enables various features of UAV. With the help of Inertial Measurement and barometric pressure sensors the horizontal level, altitude and position of UAV device can be maintained . Thus these sensors help in keeping the orientation of the UAV device stable.

These devices are embedded with the GPS module for providing autonomous flying capabilities to the UAV. These sensor enabled devices are easy to be controlled by the user and are resistant to the temperature as well as environmental changes. These MEMS devices are sometimes connected with cameras and can be used for following any person or surveillance of any area. They have excellent flying capacity and have high performance in taking reliable measurement. NB-IoT devices are used for defense purposes for surveying the battlefields and informing the officers about the necessary step that can be taken at the right time. Military vehicles are provided with sensors so that their performance can be sensed and at the time of any fluctuations, these sensors will inform the staff about it. Sensors can be attached to the soldier's clothes or with their wearable that can sense their health and can alert them about their health. Sometimes remote training by sending information in the form of video and pictures, tracking of fleet and inventory with the help of sensor embedded in the vehicle also makes a part of NB-IoT system.

Internet of things have paved many areas of military applications but securing the NB-IoT systems is the biggest threat. Security in case of defense applications is of foremost importance and necessary area to be concerned. Internet of Things has its application in Smart Home for controlling electrical and electronic devices effectively. These devices can be connected to the control systems for switching the appliances off or on during certain time when they are not required. The electrical and electronic systems are embedded with sensors and are programmed so that they can work effectively according to the requirement of the user. This will result in the enhancement of efficiency of the system and reduce the power consumption. IP cameras can be installed in our homes so that any activity can be accessed remotely through mobile phones and security of homes can be maintained. Photoelectric sensors can sense the lighting and can turn off and on whenever required.

If any smart home system is hacked by the intruder then it can get access to our private information very easily. Similar is the case with the Smart Cities. Street Lights are controlled with the help of Sensors. Traffic is managed with the help NB-IoT enabled Systems. IP cameras are installed everywhere in the city so that police can get the information about all the activities that are being carried out in the city. But if any intruder gets to hack the communication link, then it will be easy for enemy to know the dense area of population and to carry out any type of malicious attack that may lead to great loss. In the Architecture shown in Fig. 4, the NB-IoT system with IP cameras security surveillance at the

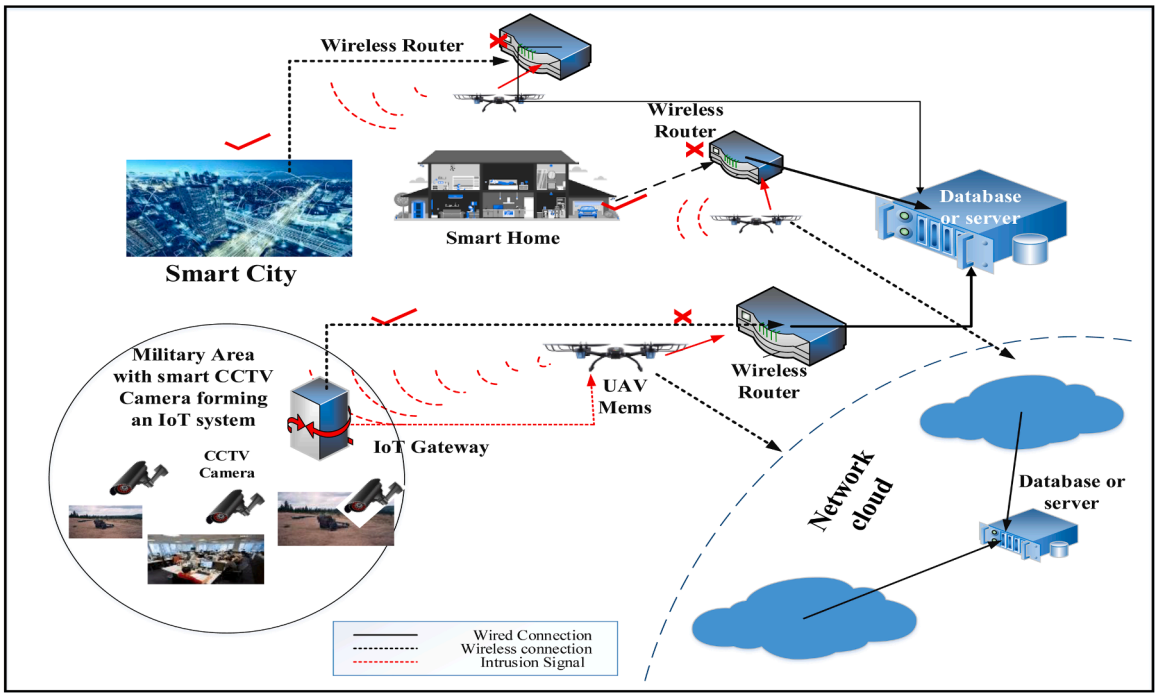

Fig. 4. Proposed architecture of security issues in NB-IoT using MEMS IoT Devices.

Perception layer surveys specific region, like Military meeting rooms, Military Control room, armory area, House's rooms, city area etc. The cameras are connected with the Internet Server through wireless router. Generally CCTV DVR have in-built Wi-Fi adapter but in some cases, CCTV DVR is connected with Ethernet port in order to connect it to the Wireless Router by forming wireless bridge.

In this network, all the information i.e. audio/ video is transmitted through a wireless connection. This Wireless connection is susceptible to be attacked by the intruder. In this case, UAV MEMS device as a BOT behaves like an intruder and tries to perform the bandwidth spoofing attack. When the BOT comes in the vicinity of Wireless Router, it will start affecting the connection and attacks the router. It tries to get all the information saved in the routing table of the router and the connection between the router and the camera gets barred. A new connection is then set up by the drone which connects the IP camera with the malicious network. The IP cameras will then start transmitting the audio/video information to the MEMS device and this further transmits all the information to the intruder. In this way, security of the system is compromised and another database rather than the conventional one can access all the information gathered by the IP cameras.

Securing NB-IoT Network is a great issue in this time. The Wi-Fi router is being used to provide access to the network and its signal strength is distributed over the network. It is very easy to get the conditions of the channel and the knowledge about the signal strength by the Eavesdropper.

The UAV BOT devices can easily monitor the nature of the router and spoof the link. By using the Game theory approach, the attacker can perform the bandwidth spoofing attack. The attacker/UAV will invite the Wi-Fi router and NB-IoT device to play the game. During the game the weakest link will get attacked. For getting the access over the link, the attacker will make use of different strategies like Prisoners Dilemma and Nash Equilibrium. By using these strategies, the Intruder will get to know the behavior as well as the strategy being used by the router.

In the game theory approach, at each iteration, probability of success is being calculated. The element with higher probability of success will win the game and get access to the channel. Let us assume that Wi-Fi router be termed as 'A', the IP camera is termed as 'B' and the UAV device/intruder be termed as 'A*'. In order to spoof the bandwidth, the intruder will invite the 'A' device to play game and apply the game theory strategies for spoofing the bandwidth.

After that the whole operation will be performed as under:

- In the First Step: The attacker is not known to the NB-IoT /IP Cameras and they will not accept any request from the Intruder or unauthorised user 'A*'. In this case, the probability of success of the intruder is very low and the connection is set up between the IP camera and the router i.e. P (A*) $<<$ P (A).
- In the Second step: After two- three iteration, the attacker starts analyzing the channel conditions and again tries to spoof the bandwidth with more efforts but this time also it cannot get the access because the probability of success of the intruder is still less than the probability of success of the router i.e. P (A*) $<$ P(A).
- In the Third step: The attacker will continue to analyze the behavior of the router and will come to know the strategy used by the router. The attacker will now make use of some better game strategy and tries to spoof the channel with more well defined manner. This time the probability of success of the attacker will be more than the probability of success of the router i.e. P (A*) $>$ P (A). With the success of the attacker, it can get access to the channel.

Thus, game theory is the strategy being used by the attacker to spoof the bandwidth and provides a serious threat to the security of NB-IoT devices.

4.1. Mathematical modeling

For analyzing the security of a smart home system, we perform the evaluation of secrecy capacity and secrecy outage probability of the proposed system model. The complexity of the channel is compared in ideal conditions and after an eavesdropper has intruded in the channel [6]. Considering a smart home scenario, the Access point (AP) allocates the channel to a CCTV camera in a smart home as shown in Fig. 5. The original signal received by the camera or the Smart Device (SD) is denoted as y_{ap} having a SNR δ.

During this transmission, an eavesdropper tries to intercept the channel and spoof the signal (δ) which is the original channel from AP to

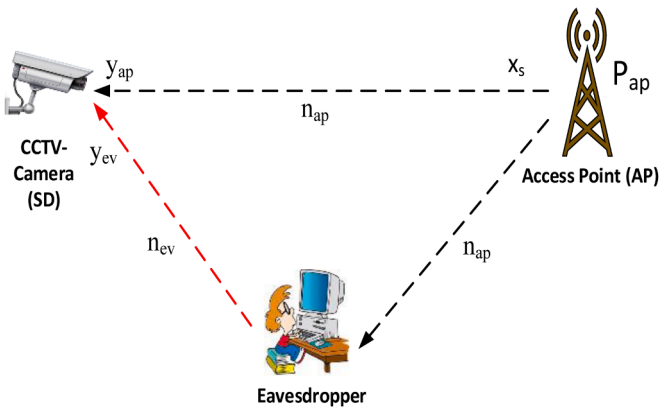

Fig. 5. Smart Device enabled attack scenario.

SD. The noise introduced by the eavesdropper is n_{ev}, because of which the signal strength received by the CCTV camera is $\delta'(\delta > > \delta')$.

Consider the original signal transmitted by the access point as x_s. The signal received at the smart device sent by the access point is

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

Where P_{ap} is the average power transmitted from the access point, h_{ap} is the channel fading coefficient from AP to SD, n_{ap} is the Additive White Gaussian Noise (AWGN) with variance σ^2_{ap}.

Simultaneously, the signal received from the eavesdropper is represented as

$$y_{ev} = \sqrt{P_{ap}} h_{ev} x_s + n_{ap} \ + n_{ev} \tag{2}$$

The wireless channel fading coefficient from the eavesdropper to SD is h_{ev} and n_{ev} is the AWG noise due the eavesdropper channel having variance σ^2_{ev}.

From Eq. (1) we can compute the channel capacity between the AP and SD as follows:

$$C_{ap} = \log_2(1 + \alpha_{ap}) \tag{3}$$

The effective SINR α_{ap} is given as:

$$\alpha_{ap} = \frac{P_{ap}|h_{ap}|^2}{I + \sigma^2_{ap}} \tag{4}$$

The channel gain is depicted as $|h_{ap}|^2$and I is the interference introduced by the eavesdropper.

From Eq. (2) the channel capacity between the AP and eavesdropper is written as

$$C_{ev} = \log_2(1 + \alpha_{ev}) \tag{5}$$

The effective SINR of the eavesdropper channel is as follows:

$$\alpha_{ev} = \frac{P_{ap}|h_{ev}|^2}{I + \sigma^2_{ap} + \sigma^2_{ev}} \tag{6}$$

Considering the presence of a number of eavesdroppers, there is a cooperative attack by them simultaneously. We consider n eavesdroppers operating simultaneously for a cooperative attack and the channel capacity is given as follows:

$$C_{ev,n} = \log_2(1 + \alpha_{ev,n}) \tag{7}$$

The effective SINR is given as

$$\alpha_{ev,n} = \frac{P_{ap}|h_{evn}|^2}{I + \sigma^2_{ap} + \sigma^2_{ev_1} + \sigma^2_{ev_2} + \sigma^2_{ev_3} - - - + \sigma^2_{ev_n}} \tag{8}$$

The total SINR due to n cooperative eavesdroppers on the channel is given as $\alpha_{ev,\ n}$ and $|h_{evn}|^2$ is the channel gain. The variance due to n eavesdroppers is given as $\sigma^2_{ev_1}, \sigma^2_{ev_2}, \sigma^2_{ev_3}, \ \ldots\ldots, \sigma^2_{ev_n}$.

The secrecy capacity is computed by denoting the difference of the channel capacities between the original channel i.e. between the access point and SD and the eavesdropper's channel. With the eavesdroppers present in the system, the secrecy capacity is given as follows:

$$C_{Secrecy} = \left[C_{ap} - C_{ev}\right]^+$$

$$= \left[\log_2(1 + \alpha_{ap}) - \log_2(1 + \alpha_{ev})\right]^+$$

$$C_{Secrecy} = \begin{cases} \log_2 \dfrac{(1 + \alpha_{ap})}{(1 + \alpha_{ev})} & \alpha_{ap} > \alpha_{ev} \\ 0 & \alpha_{ap} \leq \alpha_{ev} \end{cases} \tag{9}$$

The obtained secrecy capacity is a positive value if the SINR of the original channel between the access point and the SD is greater than the SINR of the eavesdroppers channel. If the SINR of the eavesdroppers channel is more then the secrecy capacity is zero. From Eq. (9) it can be written

$$C_{Secrecy} = \begin{cases} \log_2 \dfrac{(1 + \alpha_{ap})}{(1 + \alpha_{ev})} & \alpha_{ap} > \alpha_{ev} \\ 0 & \alpha_{ap} \leq \alpha_{ev} \end{cases}$$

Substituting the values of α_{ap} and α_{ev} from Eq. (4) and (6) in the above equation we get

$$C_{Secrecy} = \begin{cases} \log_2 \dfrac{\left(1 + \dfrac{P_{ap}|h_{ap}|^2}{I + \sigma^2_{ap}}\right)}{\left(1 + \dfrac{P_{ap}|h_{ev}|^2}{I + \sigma^2_{ap} + \sigma^2_{ev}}\right)} & \alpha_{ap} > \alpha_{ev} \\ 0 & \alpha_{ap} \leq \alpha_{ev} \end{cases}$$

For n eavesdroppers operating collaboratively, the secrecy capacity can be written as follows:

$$C^n_{Secrecy} = \left[C_{ap} - C_{evn}\right]^+$$

$$= \left[\log_2(1 + \alpha_{ap}) - \log_2(1 + \alpha_{evn})\right]^+$$

$$C^n_{Secrecy} = \begin{cases} \log_2 \dfrac{(1 + \alpha_{ap})}{(1 + \alpha_{evn})} & \alpha_{ap} > \alpha_{evn} \\ 0 & \alpha_{ap} \leq \alpha_{evn} \end{cases} \tag{10}$$

In the above cooperative eavesdropper attack if the SINR of the channel between the AP and SD is greater than the SINR of the eavesdroppers channel then positive secrecy rate is obtained otherwise secrecy rate is zero and the system is compromised by the eavesdropper.

4.2. Equations for secrecy outage probability

Secrecy Outage Probability (SOP) is defined as the probability that the instantaneous secrecy capacity $C_{Secrecy}$ is less than a predetermined threshold secrecy rate Th_{sec}, (i.e., if $C_{Secrecy} < Th_{sec}$) [37]. The outage probability is given by the following equation:

$$\mathcal{P}_{out}(Th_{Sec}) = \mathcal{P}(C_{Secrecy} < Th_{Sec}) \tag{11}$$

Eq. (11) can be rewritten as

$$\mathcal{P}_{out}(Th_{Sec}) = \mathcal{P}\left(\frac{(1 + \alpha_{ap})}{(1 + \alpha_{ev})} < 2^{Th_{Sec}}\right) \tag{12}$$

The operational significance of this definition of outage probability is when secrecy rate is set more than zero i.e. $Th_{sec} > 0$.

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

$$C'_{ev} = C_{ap} - Th_{Sec}$$

Table 2
Layerwise IoT/NB-IoT Security Attack.

S. No.	Layer	Available Attacks on IoT Devices	Definition	Countermeasures	Ref.
	Layer 1-Perception Layer	Jamming Attack	Radio jamming can result in IoT devices not being able to provide services to a valid user.	Detect and sleep route around jammed regions.	[36]
		Tampering attack/ Node capturing	In this attack an eavesdropper tampers the IoT device by causing changes in the program code, hardware circuit etc. resulting in compromised security.	Hide nodes. Tamper resistant packaging.	[37]
		Eavesdropping attack	An eavesdropper intercepts the information transmitted from a base station to the IoT node and uses it for attacks in the future.	Isolating an IoT node. Restrictions in accessing the valid node.	[38]
		Tag Cloning	An attacker clones the identity of a RFID tag and uses it in place of an original tag.	Authentication algorithm for tag.	[39]]
		Node destruction attack	In this attack there is physical damage caused to a node leading to permanent destruction of it.	Guarding the nodes from physical damage by using damage-proof packaging.	[38]
		Firmware Attack	In this attack, an attacker remotely controls a device by installing a malicious firmware on it.	Using root access on IoT device system.	[40]
	Layer 2-Network Layer	Replay Attack	In this attack, there is interception and retransmission of a message repeatedly to utilize the sensor's resource.	Introduction of timestamp. Secure session key management.	[41]
		Sybil Attack	In this attack, an attacker creates a pseudo-identity and deceives the valid user hence compromising the effectiveness of the IoT system.	Comprehensive comparisons to detect Sybil. Sybil detection techniques such as SGSD based on Social Graph or BCSD on behavior classification.	[42]
		Flooding Attack	An attack floods the routes in a network with large number of packets that can cause failure in a network.	Setting a timer limit for a node to reply and if the time exceeds, the sender can be considered as an attacker.	[43]
		Black hole attack	In this, the attacker deceives by depicting that it carries the shortest route to the receiver and attracts the data traffic towards itself.	Setting a timer limit for a node to reply and if the time exceeds, the sender can be considered as an attacker. Denying route access. Detecting information of false route.	[38, 44]]
		Wormhole Attack	In this type of attack, the attacker displaces the packets from one place of the network and places them at a distant location.	Wormhole Detection methods/techniques.	[38, 44]]
		Sinkhole Attack	In this attack, the attacker deceives the other nodes by directing them towards a false route. In this way, it directs the network traffic to a pseudo destination.	Cryptographic techniques/methods. Restricting every node with data flow limit.	[45]
	Layer 3-Service Management Layer	Service Hijacking	This type of attack occurs in the lower layers where the service provider holds the responsibility of providing security of IoT services. A secure application is built by the developer but the security remains compromised due to lower layer such as Platform as a Service (PaaS) in IoT.	Fragmentation redundancy scattering.	[46]
		Third- Party relationship	When there are two or more sources of data, the security of the data and network is compromised due to greater issues. PaaS provides third-party service components in such cases called as mashup.	Encrypting source data.	[46]
		Virtualization threat	In virtualization, a virtual machine runs different applications due to which the security threat increases as there is requirement of the virtual layer to be secured.	HyperSafe approach required for hypervisor control-flow integrity.	[47]
	Layer 4- Application Layer	API Attacks	To develop a software there are a set of protocols and tools contained in the API. If the designing of the Application programming Interface is poor it can result in API attack.	Analyzing the cloud service provider interface and security model carefully. High authentication and access control required.	[48]
		DoS/ DDoS Attack	In this type of attack, the attacker sends a large number of requests to the valid node due to which the valid node loses onto a large amount of resource and does not respond to it.	Effective DDoS mitigation plans. Introducing extra filters to catch DDoS attack initially and inform the router about the attack.	[49]
		Malicious code Injection	In this attack, an attacker creates pseudo measurements in the IoT system by determining the configuration of the system which hampers the security of the system.	Regular check for similarity. Testing the system prior installing.	[50]
	Layer 5- Business Layer	Data aggregation distortion	When all the data is collected it is sent to the base station by the device for processing it further. This data can be modified or distorted by an eavesdropper /attacker before sending it further.	Protection mechanism to protect data integrity.	[46]

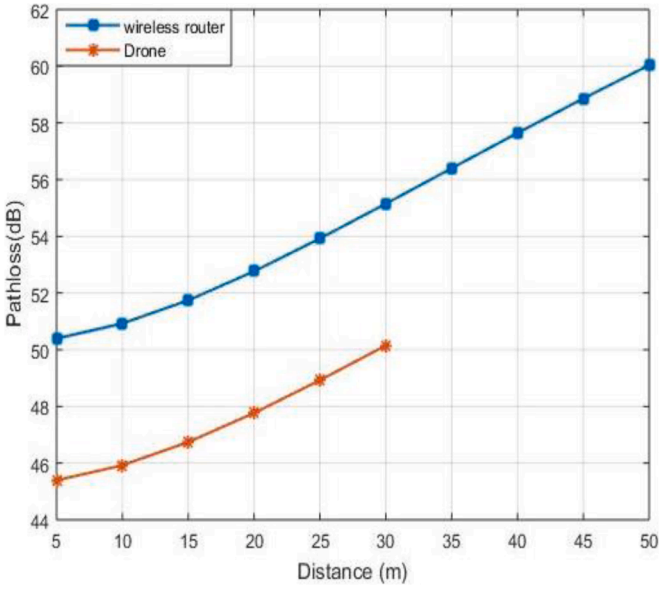

Fig. 6. Path loss v/s distance.

As, $Th_{Sec} < C_{Secrecy}$, eavesdropper channel has low capabilities than base station channel i.e. $C_{ev} < C'_{ev}$, so security of information over the channel is good. Otherwise, if $Th_{Sec} > C_{Secrecy}$, then $C_{ev} > C'_{ev}$ then information security is affected. In previous case, when noise signals are introduced by the eavesdropper. SOP will become as given under:

$$\mathcal{P}_{out}\left(C_{Secrecy} \ \langle Th_{Sec} \mid \alpha_{ap} > \alpha_{ev}\right)$$

$$= \mathcal{P}\left(\alpha_{ap} < 2^{Th_{Sec}}\ (1+\alpha_{ev}) - 1 \middle|\ \alpha_{ap}\rangle \alpha_{ev}\right)$$

$$= \int_{0}^{\infty} \int_{\alpha_{ev}}^{2^{Th_{Sec}}\ (1+\alpha_{ev})-1} \mathcal{P}(\alpha_{ap}\ , \alpha_{ev} \left| \alpha_{ap} > \ \alpha_{ev} \right.) d\alpha_{ev} d\alpha_{ap}$$

$$= \int_{0}^{\infty} \int_{\alpha_{ev}}^{2^{Th_{Sec}}\ (1+\alpha_{ev})-1} \frac{\mathcal{P}(\alpha_{ap}\ \mathcal{P}(\alpha_{ev})}{\mathcal{P}(\alpha_{ap} > \alpha_{ev}\ )} d\alpha_{ev} d\alpha_{ap}$$

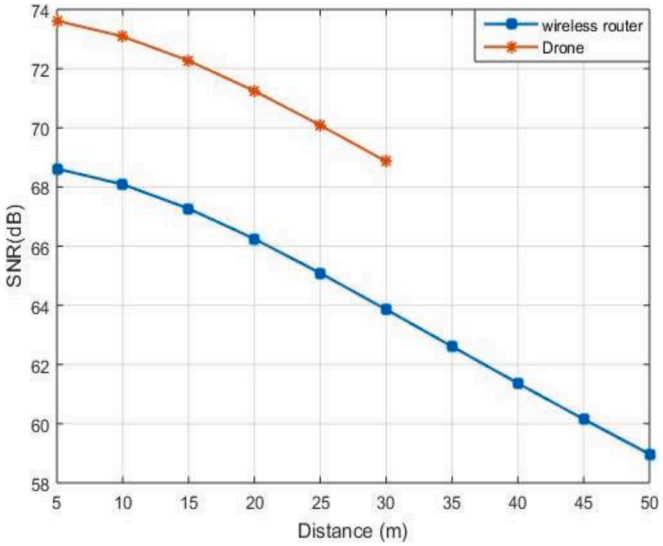

Fig. 7. SNR v/s Distance.

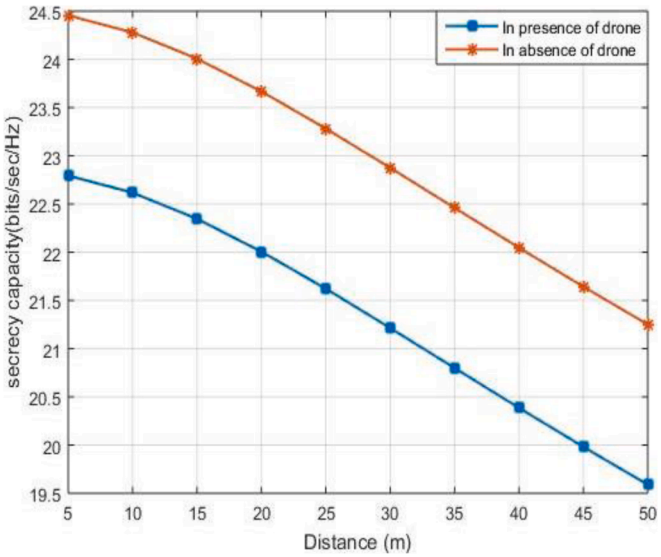

Fig. 8. Secrecy capacity v/s distance.

$$\mathcal{P}_{out}(Th_{Sec}\ ) = 1 - \frac{\overline{\alpha}_{ap} + \overline{\alpha}_{ev}}{\overline{\alpha}_{ap} + 2^{Th_{Sec}}\ \overline{\alpha}_{ev}} exp\left(- \ \frac{2^{Th_{Sec}}\ - 1}{\overline{\alpha}_{ap}} \right) \tag{13}$$

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

$$\mathcal{P}_{out}\left(C_{Secrecy} \ \langle Th_{Sec} \mid \alpha_{ap} \leq \alpha_{ev}\right) = 1$$

5. Performance analysis

In the proposed architecture, we have considered a network scenario comprising of CCTV camera surveillance System in a closed environment. The closed environment can be a hall/room involving confidential communication exchange between entities. The CCTV camera/ IP

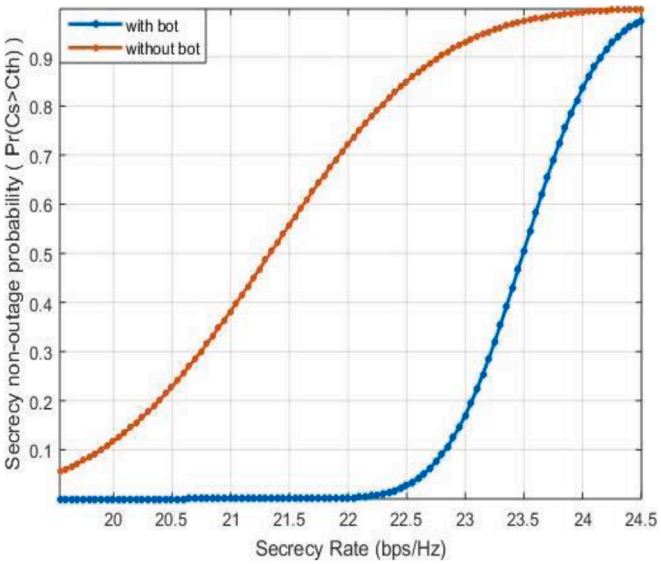

Fig. 9. Secrecy non-outage probability v/s secrecy rate.

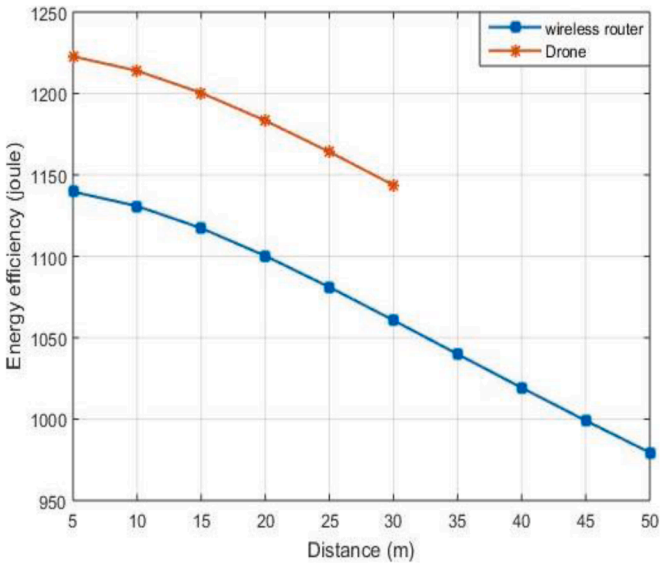

Fig. 10. Energy efficiency v/s distance.

Camera is connected through a wireless router, transferring the captured information via the internet server. In this case it is assumed that the CCTV DVR is devoid of an inbuilt Wi-Fi adapter and is connected with an Ethernet port to the wireless router forming a wireless bridge as already stated in the previous chapters. Since all the information in the network i.e. in the form of text, audio or visual is carried on a wireless network; it creates breaches in the network making it susceptible to be targeted by malicious attackers in the network. One possibility of intrusion can be BOT attack by a drone. Generally, a botnet consists of a number of devices called as bots, which consist of a malware installed that is remotely controlled by a server. As the drone comes in the vicinity of the wireless router, it starts to affect the connection of the IP camera with the wireless router and acts as a malicious node spoofing the information transmitted between them.

The drone is able to establish a stable and stronger connection as it is assumed to be operating at a higher transmitting power and at a lesser distance from the reference point (hall/room) in comparison to the wireless router. As the drone establishes a stronger and a more stable connection with the camera, the signal between the camera and the router is barred. The drone acting as an intruder in the network maintains the new connection now made. This way all the information captured in the network is directed towards the database connected to the intruder and not to the conventional database, hence compromising the security of the network.

This section discusses the result and the analysis based on the observation that have been made from the implantation of mathematical model in the proposed Architecture. The Proper analysis of security issues in the proposed architecture with malicious attack by the BOT device or UAV MEMS device is made and compared with system in which the attack is not carried. The graph in Fig. 6 depicts the comparison of path loss for the wireless router and the intruder (i.e. drone in this case) over a distance. As we know that the path loss increases proportionally with increase in distance due to decrease in the signal strength and increase in the path loss exponent due to obstructions, the plot for the same can be seen from the figure. The wireless router lies in the range of about 50 m from the reference point (i.e. IP Camera in this case) while the drone lies in the range of about 30 m from the reference.

As the drone is in close vicinity to the reference point (i.e. IP Camera in this case), the path loss values are lower for it in comparison to the router, which is at a farther distance. The carrier frequency of 2.4 GHz is used for the scenario. It is evident from the graph that the path loss values are higher for the wireless router than the drone and as the distance increases there is an exponential rise in the path loss values for both the entities. The graph in Fig. 7 depicts the plot of SNR v/s distance for the wireless router and the drone. As examined in the case of increasing path loss with increasing distance for the router and the drone the Signal to Noise ratios decrease with increasing distance.

It is evident from Fig. 7 that the drone lying at closer distance to the reference has a strong signal strength and hence high channel gain, so has a high value of SNR. Whereas in the case of wireless router lying at a farther distance, the signal strength is weak and the channel also experiences fading, multipath propagation and so on due to which the SNR decreases. The SNR values for the router correspond to the values ranging from 5 to 50 m and for the drone the values correspond to a range of 5–30 m. As the drone is acting as a malicious node and is intending to attack the integrity and confidentiality of the system to spoof the information captured, it is required to maintain a SNR value higher than the router. In the given scenario, originally, the wireless router receives all the information captured by the IP Camera, but as there is an intruder in the network i.e. the drone that is acting as an

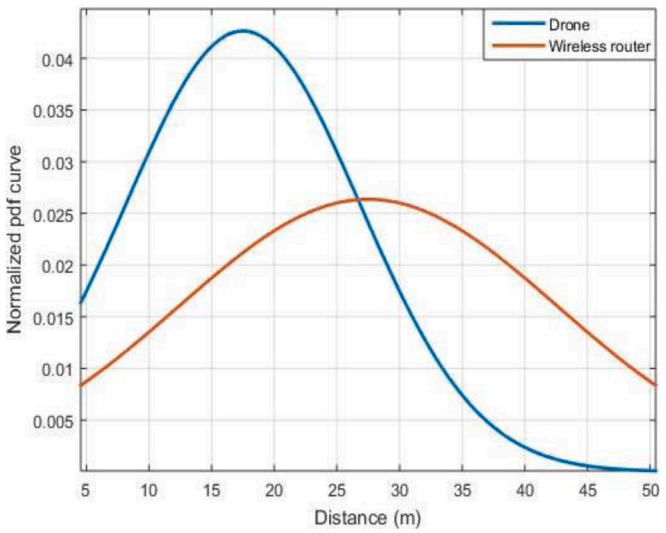

Fig. 11. Normalized pdf curve v/s distance.

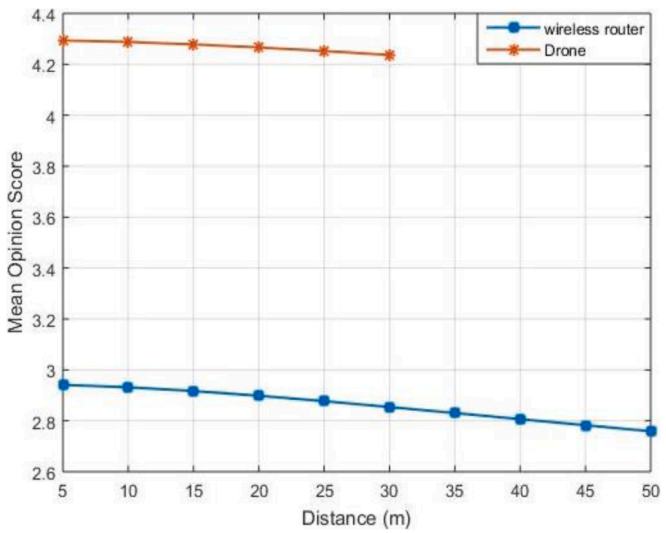

Fig. 12. Mean Opinion score v/s distance.

eavesdropper, the secrecy of the original data carried in the network has to be maintained. The graph in Fig. 8, depicts the scenario of the network in presence and absence of an eavesdropper in terms of achievable secrecy capacity.

Secrecy capacity is a measure of the difference in capacity of the main channel and the eavesdropper channel in the network. It is required that the secrecy capacity to be a high value even in the presence of an attacker so that the confidentiality of the data is maintained. From Fig. 8 it is observed that with increase in the distance up to 50 m, the secrecy rate in absence of the drone is expected to be in the range of 24.5 to 21.25 bits/s/Hz, while as in presence of an eavesdropper the secrecy rate is expected to drop from 22.25 to 19.5 bits/s/Hz. The drop in the secrecy rate creates a threat to the integrity, confidentiality, privacy and non-repudiation of the network.

Fig. 9 depicts the graph for non-outage probability of the network v/s the secrecy rate. From the graph it is evident that the malicious attacker is certain to experience lower path loss in comparison to the legitimate user. Consequently the secrecy capacity is expected to be decreased by the nearest malicious attacker, such that probability of the secrecy rate of the source to destination channel is greater than specified threshold denoted by C_{th} known as secrecy non outage probability, given as: $P_r(C_s > \ Th_{sec}) = P_r\left[log_2\left(\frac{r^{-1}+\alpha_l^{-\theta}}{r^{-1}+\alpha_e^{-\theta}}\right) > \ Th_{sec}\right]$ In the above expression C_s denotes the capacity of the main channel and Th_{sec} denotes the threshold value of the secrecy capacity. θ denotes the path loss exponent, α_l is the distance between the target node i.e. the legitimate user and the serving node (i.e. CCTV Camera). α_e is the distance between serving node and the eavesdropper. $'r'$ is the ratio of power densities of transmit signal and noise respectively.

From Fig. 9 we analyze the secrecy non-outage probability is defined under the assumption that the malicious attacker has a perfect knowledge about the location of the wireless router and state of the channel. The non-outage probability is observed to be increased with an increase in secrecy rate. In presence of an eavesdropper the secrecy outage probability is a lower value in comparison to the outage probability obtained without a bot in the network.

Fig. 10 denotes the graph for energy efficiency v/s distance. The energy efficiency of the drone is higher than that of the wireless router as the throughput and the SNR values are much higher for the drone in comparison to the router. As the distance increases there is a significant drop in the energy efficiency and can be observed from the graph. This high energy efficiency values for the drone helps it maintain a strong and stable connection with the reference point so that information can be spoofed from the reference. Fig. 11 depicts the graph depicting the normalized pdf curve v/s distance for the drone and the router.

It is observed from the graph that the signal strength of the drone is greater as compared to the wireless router as the distance lies in the range of 30 m for drone, which increases the strength of the signal. For the wireless router the distance lies in the range of 50 m, where the evaluated value of signal strength is lower as compared to drone. Therefore, the possibility of connecting the drone with the serving node is higher as compared to the wireless router.

Fig. 12 depicts the graph for the mean opinion score v/s distance. The mean opinion score is a measure of the Quality of experience of the user. The values vary on a scale of 1–5, with 1 being the worst quality of experience and 5 the best quality of experience. MOS values obtained are higher for the drone as for the wireless router. The values range between 3 and 2.8 for the wireless router and for the drone it ranges between 4.3 and 4.2. Better experience is observed for the drone as it has a higher strength in comparison to the router because the drone is operating at a much closer distance from the reference point. The simulation results validate that a UAV MEMS bot can successfully spoof the information from a valid network. Intelligent models based on artificial intelligence and efficient Intrusion detection systems are required to remove such anomalies from the network.

6. Conclusion

This article addresses an area of concern for the upcoming Narrow Band Internet of Things (NB-IoT) network. As this area is growing with the advancement in technology, security of the data transmitted and received using NB-IoT needs to be addressed. This paper presents a detailed analysis of security attacks in a NB-IoT structure with layer wise description of the security concerns at each level. The major areas i.e. defense security and security in particularly addressed, as they need high security of data. A novel proposal is presented that depicts the security attacks that can take place due a UAV MEMS device, as it is very small. A case study is presented that discusses the proposal with the performance analysis comprising secrecy rate and secrecy outage probability analysis. The results validate that a bot can efficiently spoof the valid data from the network and the entire security will be compromised. The future NB-IoT networks need to be made more secure and intelligent solutions based on machine learning, prediction models, Game Theory are required for formulating efficient Intrusion Detection System (IDS) to detect and prevent malicious security attacks in a NB-IoT system.

Author statement

All persons who meet authorship criteria are listed as authors, and all authors certify that they have participated sufficiently in the work to take public responsibility for the content, including participation in the concept, design, analysis, writing, or revision of the manuscript. Furthermore, each author certifies that this material or similar material has not been and will not be submitted to or published in any other publication before its appearance in Computer Networks Journal

Authorship contributions

Please indicate the specific contributions made by each author (list the authors' initials followed by their surnames, e.g., Y.L. Cheung).

Declaration of Competing Interest

There is no conflict of interest for this work.

Acknowledgements

All persons who have made substantial contributions to the work reported in the manuscript (e.g., technical help, writing and editing assistance, general support), but who do not meet the criteria for authorship, are named in the Acknowledgements and have given us their written permission to be named. If we have not included an Acknowledgements, then that indicates that we have not received substantial contributions from non-authors.

References

[1] S. Popli, R.K. Jha, S. Jain, A survey on energy efficient Narrowband Internet of things (NBIoT): architecture, application and challenges, IEEE Access 6 (2018) 1–34. Nov.
[2] E. Rastogi, N. Saxena, A. Roy, D.R. Shin, Narrowband Internet of Things: a comprehensive study, Computer Netw. (2020), https://doi.org/10.1016/j.comnet.2020.107209.
[3] Y.D. Beyene, R. Jantti, O. Tirkkonen, K. Ruttik, S. Iraji, A. Larmo, T. Tirronen, J. Torsner, NB-IoT technology overview and experience from cloud-RAN implementation, IEEE Wirel. Commun. 24 (3) (2017) 26–32. June.
[4] X. Yang, X. Wang, Y. Wu, L.P. Qian, W. Lu, H. Zhou, Small-cell assisted secure traffic offloading for Narrowband Internet of Thing (NB-IoT) Systems, IEEE IoT J. 5 (3) (2018) 1516–1526. June.
[5] R. Boisguene, S.C. Tseng, C.W. Huang, P. Lin, A survey on NB-IoT downlink scheduling: issues and potential solutions, in: International Wireless Communications and Mobile Computing Conference, 2017, pp. 547–551. June.
[6] V. Kumar, R.K. Jha, S Jain, NB-IoT security: a survey, Wirel. Pers. Commun. (2020), https://doi.org/10.1007/s11277-020-07346-7.

[7] V. Hassija, V. Chamola, V. Saxena, D. Jain, P. Goyal, B. Sikdar, A survey on IoT security: application areas, security threats, and solution architectures, IEEE Access 7 (2019) 82721–82743.

[8] I.U. Din, M. Guizani, B.-S. Kim, S. Hassan, M.K. Khan, Trust management techniques for the Internet of Things: a survey, IEEE Access 7 (2019), 29763-29787.

[9] S. Kumar, S. Sahoo, A. Mahapatra, A.K. Swain, K.K. Mahapatra, Security enhancements to system on chip devices for IoT perception layer, Proc. IEEE Int. Symp. Nanoelectron. Inf. Syst. (iNIS) (2017) 151–156. Dec.

[10] C.-H. Liao, H.-H. Shuai, L.-C. Wang, Eavesdropping prevention for heterogeneous Internet of Things systems, in: Proc. 15th IEEE Annu. Consum. Commun. Netw. Conf. (CCNC), 2018, p. 1_2. Jan.

[11] APWG. Phishing Activity Trends Report. Accessed: Feb. 12, 2019. [Online]. Available:https://docs.apwg.org/reports/apwg_trends_report_q4_2017.pdf.

[12] C. Li, C. Chen, A multi-stage control method application in the _ght against phishing attacks, in: Proc. 26th Comput. Secur. Acad. Commun. Across Country, 2011, p. 145.

[13] C. Kolias, G. Kambourakis, A. Stavrou, J. Voas, DDoS in the IoT: mirai and other botnets, Computer (Long Beach Calif) 50 (7) (2017) 80_84.

[14] M.A. Razzaque, M. Milojevic-Jevric, A. Palade, S. Clarke, Middleware for Internet of Things: a survey, IEEE Internet Things J. 3 (1) (2016) 70_95. Feb.

[15] WS-Attacks. Attack Subtypes. Accessed: Feb. 9, 2019. [Online]. Available: https://www.ws-attacks.org/XML_Signature_Wrapping.

[16] S.N. Swamy, D. Jadhav, N. Kulkarni, Security threats in the application layer in IoT applications, in: Proc. Int. Conf. IoT Social, Mobile, Analytics Cloud (I-SMAC), 2017, pp. 477–480. Feb.

[17] H.A. Abdul-Ghani, D. Konstantas, M. Mahyoub, A comprehensive IoT attacks survey based on a building-blocked reference model, Int. J. Adv. Comput. Sci. Appl. 9 (3) (2018) 355–373.

[18] Q. Jing, Security of the Internet of Things: perspectives and challenges, Wirel. Netw. 20 (2014) 2481–2501. Nov.

[19] K. Meynell, OTA & IoT: a shared and collaborative responsibility, in: APAN 46 Meeting, Auckland, 2018.

[20] H. Sedjelmaci, A hierarchical detection and response system to enhance security against lethal cyber-attacks in UAV networks, IEEE Trans. Syst. Man Cybern. Syst. 48 (2018) 1594–1606. Sept.

[21] N.H. Motlagh, UAV-based IoT platform: a crowd surveillance use case, IEEE Commun. Mag. 55 (2017) 128–134. Feb.

[22] H.Y. Tsai, M. Siebenhaar, A. Miede, Y. Huang, R. Steinmetz, Threat as a service?: virtualization's impact on cloud security, IEEE J. IT Prof. 14 (1) (2012) 32–37. Feb.

[23] N.K.J. Mosenia, A comprehensive study of security of Internet-of-Things, IEEE Trans. Emerg. Top. Comput. 5 (4) (2017) 586–602. Oct.–Dec.

[24] Z. Ling, J. Luo, Y. Xu, C. Gao, K. Wu, X. Fu, Security vulnerabilities of internet of things: a case study of the smart plug system, IEEE Internet Things J. 4 (6) (2017) 1899–1909. Dec.

[25] https://www.credencys.com/blog/internet-of-things-the-agent-of-change-for-the-defense-system/.

[26] D. Mocrii, Y Chen, P Musilek, IoT-based smart homes: a review of system architecture, software, communications, privacy and security", Internet Things 1–2 (2018) 81–98. VolumesSeptember.

[27] S. Hayat, E. Yanmaz, R. Muzaffar, "Survey on unmanned aerial vehicle networks for civil applications: a communications viewpoint.

[28] H. Shakhatreh, A. Sawalmeh, A. Al-Fuqaha, "Unmanned aerial vehicles: a survey on civil applications and key research challenges", arXiv: 1805.00881 v1 [cs.RO] 19 Apr 2018.

[29] A. Gupta, R.K. Jha, P. Gandotra, S. Jain, Bandwidth spoofing and intrusion detection system for multistage 5G wireless communication network, IEEE Trans. Veh. Technol. 67 (1) (2018) 618–632. January.

[30] S. Garg, K. Kaur, G. Kaddoum, J.J.P.C. Rodrigues, M. Guizani, Secure and lightweight authentication scheme for smart metering infrastructure in smart grid, IEEE Trans. Ind. Inf. 16 (5) (2020) 3548–3557. May.

[31] M.A. Akram, K. Mahmood, S. Kumari, H. Xiong, Comments on "Toward secure and provable authentication for internet of things: realizing industry 4.0", IEEE Internet Things J. 7 (5) (2020) 4676–4681. May.

[32] N. Neshenko, E. Bou-Harb, J. Crichigno, G. Kaddoum, N. Ghani, Demystifying IoT security: an exhaustive survey on IoT vulnerabilities and a first empirical look on internet-scale IoT exploitations, IEEE Commun. Surv. Tutor. 21 (3) (2019) 2702–2733, thirdquarter.

[33] S. Garg, K. Kaur, N. Kumar, G. Kaddoum, A.Y. Zomaya, R. Ranjan, A hybrid deep learning-based model for anomaly detection in cloud datacenter networks, IEEE Trans. Netw. Serv. Manage. 16 (3) (2019) 924–935. Sept.

[34] P. Illy, G. Kaddoum, C.M. Moreira, K. Kaur, S. Garg, Securing fog-to-things environment using intrusion detection system based on ensemble learning, in: IEEE Wireless Communications and Networking Conference (WCNC), Marrakesh, Morocco, 2019, pp. 1–7, 2019.

[35] M. binti Mohamad Noor, W.H. Hassan, Current research on Internet of Things (IoT) security: a survey, Comput. Networks 148 (2019) 283–294.

[36] N. Namvar, W. Saad, N. Bahadori, B. Kelley, Jamming in the Internet of Things: a game-theoretic perspective, in: IEEE Global Communications Conference (GLOBECOM), 2016, pp. 1–6.

[37] S.H. Jokhio, I.A. Jokhio, A.H. Kemp, Node capture attack detection and defense in wireless sensor networks, IET Wirel. Sens. Syst. 2 (3) (2012).

[38] A. Mosenia, N.K. Jha, A comprehensive study of security of Internet-of-Things, IEEE Trans. Emerg. Top. Comput. 5 (4) (2017) 586–602, 1 Oct.-Dec.

[39] J. Abawajy, Enhancing RFID tag resistance against cloning attack. Third International Conference On Network and System Security, Gold Coast, QLD, 2009, pp. 18–23, 20092009.

[40] Z. Ling, J. Luo, Y. Xu, C. Gao, K. Wu, X. Fu, Security vulnerabilities of Internet of Things: a case study of the smart plug system, IEEE Internet Things J. 4 (6) (2017) 1899–1909. Dec.

[41] Y. Feng, W. Wang, Y. Weng, H. Zhang, 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, 2017, pp. 541–547.

[42] K. Zhang, X. Liang, R. Lu, X. Shen, Sybil attacks and their defenses in the Internet of Things, IEEE Internet Things J. 1 (5) (2014) 372–383. Oct.

[43] S. Manda1, Dr Nalini, Denial-of-service or flooding attack in IoT routing, Int. J. Pure Appl. Math. 118 (19) (2018) 29–42. VolumeFeb.

[44] S. Benzarti, B. Triki, O. Korbaa, Survey on attacks in Internet of Things based networks, in: 2017 International Conference on Engineering & MIS (ICEMIS), 2018. Feb.

[45] A. Salehi S., M.A. Razzaque, P. Naraei, A. Farrokhtala, Detection of sinkhole attack in wireless sensor networks, in: IEEE International Conference on Space Science and Communication (IconSpace), 2013, pp. 361–365, 1-3 July.

[46] K. Hashizume, D.G. Rosado, E.F. Medina, E.B. Fernandez, An analysis of security issues for cloud computing, J. Internet Serv. Appl. (2013).

[47] K. Xu, X. Zhang, M. Song, J. Song, Mobile mashup: architecture, challenges and suggestions, in: International Conference on Management and Service Science, Wuhan, 2009, pp. 1–4, 2009.

[48] H. Shah, S.S. Anandane, Shrikanth, "Security issues on cloud computing," arXiv: 1308.5996, Aug 2013.

[49] A. Aris, S.F. Oktug, S.B.O. Yalcin, Internet-of-Things security: denial of service attacks, in: Signal Processing and Communications Applications Conference (SIU), 2015.

[50] V.P. Illiano, E.C. Lupu, Detecting malicious data injections in event detection wireless sensor networks, IEEE Trans. Netw. Serv. Manage. 12 (3) (2015) 496–510. Sep.

Dr. Rakesh K. Jha (S'10, M'13, SM 2015) is currently an Associate Professor in 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. Received his PhD degree from NIT Surat, India in 2013.He has published more than 51 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 router of Wireless Communication has been accepted by ITU (International Telecommunication Union) in 2010. He has received young scientist author award by ITU in Dec 2010. He has received APAN fellowship in 2011,2012, 2017 and 2018 and student travel grant from COMSNET 2012. He is a senior member of IEEE, GISFI and SIAM, International Association of Engineers (IAENG) and ACCS (Advance Computing and Communication Society). He is also member of ACM and CSI, many patents and more than 3001 Citations in his credit.

Puja received the B.E. Hon's degree in Information Technology from RGPV; Bhopal in 2011.She is currently pursuing the M. Tech degree in School of Computer Science Engineering at Shri Mata Vaishno Devi University, Katra, Jammu and Kashmir, India. Her research interest includes the emerging technologies of IoT, NBIoT. Currently she is doing her research work in Security issues in IoT and Wireless Communications.

Haneet Kour (S'17) received the B.E. degree in electronics and communication engineering from Jammu University, Jammu and Kashmir, India, in 2015 and the M.Tech degree in Electronics and Communication Engineering from Shri Mata Vaishno Devi University in 2017. She is currently pursuing the Ph. D degree in Electronics and Communication Engineering at Shri Mata Vaishno Devi University, Katra, Jammu and Kashmir, India Her research interest includes the emerging technologies of 5G wireless communication network. Currently she is doing her research on Power Optimization in next generation networks. She is working on Matlab tools for Wireless Communication. She is a student member of Institute of Electrical and Electronics Engineers (IEEE).

Manoj Kumar Assistant Professor in School of Computer Science Engineering. He has. received M. Tech. & B. Tech. in the area of Computer Science and Engineering from Kurukshetra University, Kurukshetra. He is pursuing PhD in the area of Wireless Mesh Networks from SMVD University, Katra India. He has more than 14 years of experience in teaching the engineering students at undergraduate and postgraduate level. He has also guided several M. Tech. thesis and B. Tech. projects. He has published several research papers in peer reviewed international journals and conferences.

Shubha Jain is currently pursuing her Masters in Telecommunications from the University of Maryland, College Park, USA. She received her Bachelors in Electronics and Telecommunications from SGSITS, Indore, India.