A survey on ultra-dense network and emerging technologies: Security challenges and possible solutions

Garima Chopra, Rakesh Kumar Jha, Sanjeev Jain

Department of Electronics and Communication Engineering, Shri Mata Vaishno Devi University, J & K, India

Department of Computer and Communication Engineering, Shri Mata Vaishno Devi University, J & K, India

Keywords: UDN, Security, D2D, Jamming, Massive MIMO

Abstract

The recent advancements in the field of next generation mobile communication provide scope to a variety of new areas by connecting various devices through a common platform for data transfer. The addition of several applications like e-health monitoring, smart homes, surveillance etc can be managed from a remote location. It not only opens the door for new researches but also boosts the requirement to secure the network from the eye of the potential attackers. In this paper, a detailed survey has been done on security issues and their possible solutions in Ultra Dense Networks for 5G wireless network architecture. With this, a detailed explanation about security issues of physical layer in Massive MIMO, Jamming, VANET and D2D have been provided with best efforts. Also, the description about the security flaws of spectrum shared, IoT devices have been explained. At the end, the architecture for security attacks in UDN has been proposed with proper thought process in the increasing order of their risk factor.

1. Introduction

With the advent of new technologies and the growing need to provide better services having less latency, data rates having the aim to utilize spectrum to its peak, mobile generations have been growing as the new devices are merging with the existing architecture. However, a gradual but steady increase in the previous generations of mobile wireless communication have witnessed by the users. The addition of new multimedia application having a maximum of video traffic generated by mobile units like video conferencing, live video streaming, e-health applications etc raised many issues related to security or the integration among themselves. The next generation wireless communication (5G) is expected to release 1 TB of data yearly by 2020. The new devices are merging with the existing architecture. However, a gradual but steady increase in the previous generations of mobile wireless communication have witnessed by the users. The addition of new multimedia application having a maximum of video traffic generated by mobile units like video conferencing, live video streaming, e-health applications etc raised many issues related to security or the integration among themselves. The next generation wireless communication (5G) is expected to release 1 TB of data yearly by 2020. The coming 5G architecture have many new technologies to embed such a large density of devices under a single cell deployed. It consists of small homogeneous network clubbed together to form heterogeneous networks resulting in the formation of UDN with one Macrocell BS serving huge variety of small cell BS's. Hence the primary objective in the 5G architecture is to satisfy such huge traffic due to exponential growth of users under one roof. The frequency band from 300 MHz to 3 GHz is utilized till LTE networks.

However, the deployment of UDN in the practical cases need to face a lot of interference challenges due to dense and irregular transmissions. In spite of already mentioned task another area of concern is the promise from the operation to provide safe delivery of data of the users. Hence, in UDN security challenge is also a major concern for the researchers so as to provide safe passage for transmission provide better Quality of service and spectral efficiency. The densification is done up to a point where the cells are so closely associated that each cell overlaps with the two or more cells and on the ideal basis where each UE is entertained by one (or more) AP. For the previous generations of mobile communication, the security threats were not prevalent or dominant to the users. But assigning IP based architecture have exposed the network to the sight of eavesdropper with the addition of many new benefits. Instead of interference issue, energy efficiency also serves as a major parameter of interest for researchers as...
UDN architecture will add an tremendous amount of complexity at the AP side.

The requirement of high data rate provides a new insight into the use of new spectral frequency ranging from 3 GHz to 30 GHz. So the 5G architecture boosts the use of millimeter wave technology with the growing demand in data traffic. This increase in demand is motivated by the deployment of small cells from the traditional macro hexagonal coverage area. 5G architecture is based on user-centric networking where user is no longer present to only extract the benefit from the network rather it indulges in storage, relaying purpose, computational purpose etc. The specific areas of UDN deployments like malls, office, academic regions etc. In such a dense environment, direct path provides better results than the NLOS and due to mm-wave penetration in outdoor regions Direct path is preferred because in long range communication attenuation problem is more prevalent.

In the wired networks, the nodes are having a physical connection among themselves. In contrast, the wireless networks are exposed to many vulnerabilities due to broadcast nature of the medium. Hence, exposing the network to eavesdropping, DoS, spoofing etc results in the compromise of keys having a requirement of computational capability. But encryption based protection can be applicable to only limited area. Hence stress on physical layer security is laid upon or cross-layer security for protection against the user because we cannot forever assume that the adversary has limited resources (Trappe, 2015). He/she could be very well equipped with good computational power and one major weak area of using encryption is the keys exchange between nodes. Another concern is the reduction in the quality of service like throughput, delay etc which is very difficult to compromise where everyone wants to get a better service and hence requires a proper balancing. Thus physical layer security is emerging as a popular means for providing protection in wireless networks.

The major concern for security requirement arises in 4G with the introduction of All-IP based network architecture having an advantage of distributed RNC and BSC functionality distributed among eNB's, gateways etc. Major threats regions in 4G architecture is the inter-network GSM and UMTS, IP-based attacks, jamming based DoS, MITM attack, network impersonation. However, threats have been continuous growing with the increase in the density of users in which adversary tries to explore the potential weaknesses present in the architecture.

The 5G should incorporate special features lacking in LTE-A having supported capability for high speed trains up to 350 km/h. In this paper, we proposed potential security loopholes present in 5G network scenarios especially for UDN deployment. In Fig. 1, the evolution of dense network have been provided with the requirement of subscriber data, user throughput, spectrum and Machine-to-Machine/user from traditional network to Ultra dense network. Simultaneously, along with each generation basic features are presented.

1.1. Contribution

The contribution of this paper is to represent security issues related to UDN in 5G scenario. In the first section physical layer is described and the associated technologies with it. Taking one by one, the areas of physical layer like Massive MIMO, Jamming etc security issues associated with it are described with the best efforts to provide security solutions. Further, possible attacks associated with UDN are described on the increase in the density of users and the possible solutions (or work done) till date are presented. We have also tried to summarize the general and security challenges linked when UDN networks are deployed.

2. Security issues in emerging technologies

The physical layer is the lowest most layer and linked with the devices which are present in the network. We can say that it provides real interface and all the data are directed in the form of electrical pulses. In a wireless network, the information is broadcast to the outside world. Hence it is susceptible to many vulnerabilities causing many attackers to interfere with the ongoing process. Many new technologies are introduced or added with the physical layer. The introduction of massive MIMO in place of MIMO to increase the data rate. With the addition, there comes a lot of possibilities of attacks. In comparison to conventional low mobility channels, the high mobility networks are having high possibility of large fading and making the passage of intruder easy for further attack cases. However, from the method of cryptography physical layer security offers two major advantages. Firstly, the cryptography technique offers major computational complexity to physical layer. Secondly, due to high scalability of physical layer in 5G networks (Yang et al., 2015). The large number of devices need to share keys for exchanging data among themselves. As a result of this, the key distribution becomes cumbersome some process. To cope with the challenge of key distribution physical layer offers direct secure connection and could help in the security of upper layers (Yang et al., 2015). Various new devices are added in the conventional network architecture of mobile network where it leads to the development of heterogeneous network which is based on mm-wave technology having high operating frequency range and also the installation of massive MIMO which is discussed before.

2.1. Massive MIMO

Massive MIMO is emerging technology in 5G with the objective of providing high energy efficiency, robustness and spectrum efficiency (Gupta and Jha, 2015). It contains array of antennas serving many users at a time. Both the receiver and the transmitting end have hundred of antennas. This is based on spatial multiplexing and also provides CSI for both Up-link and Down-link communication. The most achievable attacks on the physical layer is the eavesdropping and jamming attacks and it can affect this layer to a great extend. The CSI of different pilot carriers are estimated when the quantized value of the terminal is feedback to the base station. When the antennas increases in the massive MIMO, more slots are needed for the storage of uplink information. The above issue is resolved with the use of Time Division Duplexing (TDD) (Gupta and Jha, 2015). Moreover, the high performance gain of massive MIMO can be achieved by the beamforming technique like Maximum Ratio transmission (MRT) and Zero forcing (ZF) where the energy is radiated in a particular intended region in comparison to MIMO. Physical layer security can be seen as the addition to the earlier cryptographic techniques which only exploits the features of channel based on the randomness. However, it is expected that the future 5G technology should be associated with low power, spectrum efficiency etc linked with the green communication. Massive MIMO proves as a promising technology in this regards. It provides a great reduction in radiated energy and hence supporting the
performance of system for low power UEs and cells with low power BSs deployed in it. Most of the traffic generated approximately 70% is indoor traffic.

2.1.1. Possible attacks and suggested solutions to massive MIMO attacks

The performance in massive MIMO is improved when transmitter and receiver antennas experiences independent fading which is derived by the value of channel coefficients (Bogale and Le, 2016). When the distance between two antennas is minimum 0.5\(\lambda\) experiences independent fading where \(\lambda\) represents wavelength of the transmitted wave (Bogale and Le, 2016). The main attack which is popular and has a high possibility is eavesdropping, jamming or DoS. To protect the network against eavesdropper especially physical layer parameters there are various methods. Firstly, the parameter called RPS (Radiated Power Scaling) is selected of the transmitted power with random number of BS and adjustment is done optimally. Secondly, the assumption is made that the state of the channel is perfect and having finite eavesdropper (Chen et al., 2016a). When physical layer security is analyzed one factor is considered in it called secrecy capacity which is the difference between channel capacity and wiretap channel. There are many techniques proposed when the value of secrecy rate goes below zero are: 1. Artificial Noise-Aided Security, 2. security-oriented beam-forming and 3. security oriented diversity approaches (Zou et al., 2016). It is seen that positive secrecy rate still can be achieved with low cost with power scaling when eavesdropper antennas are less than a particular threshold value where the other effects or factors like pilot contamination, sequence of power carrier or data stream power are considered (Chen et al., 2016a).

Below are the detailed discussion of techniques used when SR drops below zero:

2.1.1.1. Artificial noise aided security

The artificial noise aided security provides provision on the source node side to add the interfering signal to the transmitted signal. The main aim is to provide protection from the eavesdropper by making it inconvenient to intercept the signal. But for the destination node, its quite easy to recover the signal. Earlier, it is quite easy to intercept the symbols just by seeing the strength of the signal. Hence, it maintains a quite level of secrecy rate improvement by reduction in the wiretap channel capacity.

In this paper, Goel and Negi (2008) it is suggested to use the deployment of multiple antennas for the generation of artificial noise. It is also said that if the transmitter antennas are higher than that of eavesdropper then artificial noise method will not affect the performance of the desired channel. A small amount of transmitted power is required for the generation of artificial noise. It is further observed that as the population of eavesdropper increases more power is required for the generation of AN. The suggested solution below is given based on the previously aided methods when the problems were encountered in 3G onward. One scheme is proposed for MISOME wiretap channel with the assumption that source has perfect CSI and no idea about the CSI of the eavesdropper channel (Nguyen and Shin, 2011). The authors tried to optimize the value of secrecy rate with the respect to original signal and co-variance of the artificial noise. Another alternative to multiple antennas is the use of cooperative relays whose presence is required for producing artificial noise. A new protocol is proposed called secret wireless communication where relays are used for producing AN and another set of relays for transmitting message from source nodes. However, by exploiting the degrees of freedom by multiple transmitting antennas, the position of AN can be adjusted through spatial beamforming technique for maximizing the secrecy performance. Using water filling algorithm for power allocation scheme for massive MIMO to set the lower bound for secrecy rate was derived (Tsai and Vincent Poor, 2014). The performance metrics for fast and slow fading channel are explored in Zhou et al. (2010) and Zhang et al. (2013). The secrecy outage probability and Ergodic secrecy rate are used as a performance metrics for slow and fast fading channels respectively.

Considering, the case of Multi-user and Multi-eavesdropper in a macro-cell having only one BS and M users as shown in Fig. 2. Here M users are trying to transmit the data to the BS in the presence of eavesdroppers where \(U(1), U(2), ..., U(M)\) represents Mth user.

Signal received at BS can be represented as

\[ Y_B = \sqrt{P_M} H_{BM} X_M + N_0 \]  

\[ C_M = \log_2 \left( 1 + \frac{|H_{BM}|^2 P_M}{N_0} \right) \]  

Similarly for eavesdropper, the received signal would be

\[ Y_{BE} = \sqrt{P_{ME}} H_{ME} X_{ME} + N_e \]  

\[ C_{ME} = \log_2 \left( 1 + \frac{|H_{ME}|^2 P_{ME}}{N_e} \right) \]  

\[ \text{SR} = C_M - C_{ME} \]  

From Eq. (5), it can be seen that Secrecy Rate depends on the capacity of both Main channel and Eavesdropper and it is equivalent to the different of channel capacity of User and Eavesdropper (Table 1).

The consideration level of secrecy capacity is not dependent on power of the transmitted signal which increases with increase in power of the signal. Thus assigning the transmit power according to the

![Fig. 2. General scenario for possible attacks in Massive MIMO.](image-url)
channel state in wiretap and wireless for achieving optimized value of secrecy rate. A threshold can be set for the power allocation based on the full information available to main channel and partial CSI for eavesdropper which is implemented in on-off mode (Nguyen and Shin, 2011). With the addition of such a huge number of devices to the 5G network, the requirement of green communication has become an important performance criteria where the ratio of secrecy rate to power consumption is used as an evaluating method for testing the success rate of some algorithm (Zou et al., 2014). Energy-efficient power allocation scheme is a non-convex mechanism even when full CSI information is available. However, efforts have been made to reduce the complexity of power allocation using Taylor series using Eigen value decomposition in Zappone et al. (2015). In Tsai and Vincent Poor (2014), proposed an energy efficient power allocation scheme at considerably high value of SINR.

2.1.1.2. Security-oriented beamforming techniques. It is a type of beam forming techniques which is security specific in which SN transmits the information to the DN which is direction specific so that only the legitimate user is able to intercept the signal. Hence, providing protection against the eavesdropper. In the previous method of AN, the use of cooperative relays is based on the assumption of perfect CSI of the channel for that beamforming technique proves as an best alternative for the fixed transmitted power. Here, the use of AN with the combination of beamforming is proposed. Many techniques were proposed in which without depending on any knowledge about the state of wiretap channel like optimal beamforming technique (Mukherjee and Swindlehurst, 2011). As compared to AN aided security, the proposed beamforming technique performs well for moderate value of CSI with greater secrecy rate. In Chen et al. (2016a), the authors have considered the possibility that the eavesdropper might be equipped with multiple antennas and can increase the probability of interfering the signals. A scheme is proposed called OSPIR for secure transmission over the physical layer with the assumption that the eavesdropper is equipped with unlimited antennas. In this scheme, the phase of the symbol is rotated randomly before transmission at the BS. The legitimate user is able to get the correct phase whereas the eavesdropper may not be able to intercept the signals. If it does, the symbol would be full of errors irrespective of the number of antennas it is using for receiving signal. Hence, guaranteeing the security performance.

Chen et al. (2016a) it has also compared the SER of the legitimate user with the SNR for different number of base station antennas. It is observed that if the number of BS antennas increases, the value of SER of the UE improves but not much difference in value is seen for fixed BS antennas on increasing the SNR(db). OSPIR technique provides a considerable level of correlation with the green communication on increasing the amount of antennas on the BS side. In Chen et al. (2016b) paper, the authors have proposed UOSPIR scheme for IoTs devices where the possibility of power exhaustion is large during the transmission of data from devices to the eNB. They have felt the need for the protection of data in the uplink transmission which can be subjected to eavesdropper attack. Using this scheme the original symbol is rotated before transmission to the BS. It is a convenient method rather than conventional method of encryption which are complex and cannot be applied for lightweight devices. On the other hand the BS is able to infer the correct phase of the symbol, it can also be said that this scheme is a type of symbol encryption process. In UOSPIR scheme, AN issued with jamming to transmit the data for uplink and it is seen that the massive MIMO eavesdropper failed in recovering the major symbols because of its high SER on the contrary for BS having few antennas is able to get the correct symbols. For 5G data transmission where it enables the small and light weight devices into its architecture, their security is highly desired as they may be suffering from power deficiency. The introduction of massive MIMO and beamforming approach only aims for increasing the performance of the network with low costs. Hence, work on light weight encryption are required from the ground level.

2.1.1.3. Diversity-assisted security approaches. In the AN aided approaches, node (or system) uses the additional power of the BS while transmitting signals for the generation of artificial noise with the aim of improving physical layer security. Whereas the diversity assisted approach provides security without the use of additional power. Multiple-antennas diversity is based on selecting the optimal transmitting antenna based on the information of CSI of the channel and wiretap channel. Hence, maintaining the high secrecy rate. It can also be done by selecting the antenna having the highest channel capacity.

For multi-user diversity approach, the multiple users are served by BS in cellular network, OFDMA is used for communicating. Multi-user scheduling is enabled for the OFDM band for the transmitted signals. The capacity of the wiretap channel should be decreased with increase in capacity of the main channel for protection against the eavesdropper during wireless transmission. In cooperative relay diversity approach, where the best relay is selected among a group of relays.

With the deployment of massive MIMO, many design problems that were earlier present gets eliminated. When the antennas of the BS increases the problem of small scale fading diminishes, noise can be canceled or averaged, the interference issues, channel estimation errors and many hardware issues have seen a remarkable decreased value. One major challenge still exists is the pilot contamination and for the UDN deployment which requires the integration of large users need to cater to the arising problem. Hence, directly affecting the performance of Ultra-dense network by exhausting is resources by compromising the security of the users. The other alternative could be the designing of such technique which off loads the work from BS and resource exhaustion at the antenna side due to adversary impact is highly intolerable which needs to take care. It is seen that for large antennas the secrecy outage probability reduces for both ZF and MRT methods (Yang et al., 2015). But a significant variable in value are observed for both MRT and ZF. We can say that ZF dominate the MRT as the interference canceled in ZF.

2.2. Jamming attacks in wireless networks

In the previous section, we have discussed issues related to massive MIMO in physical layer. We have also tried to explain the algorithms for the prevention of eavesdropper present in various papers. The main reason for the launch of eavesdropping or other attacks is the nature of the channel which broadcasts the information in the environment. Hence, making the transmitted information more vulnerable to attacks by the adversary present in the surrounding area. Another issue which is prominent in mobile communication is the jamming attack. In the jamming attack, the attacker sends the radio signal to interfere with the communication of the legitimate node (Ozan Basciftci et al., 2016). The

---

**Table 1**

<table>
<thead>
<tr>
<th>Notation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>$Y_b$, $Y_e$</td>
<td>Received signal strength at BS and Eavesdropper respectively.</td>
</tr>
<tr>
<td>$P_{tx}$, $P_{e}$</td>
<td>Transmission power from user and eavesdropper respectively to BS</td>
</tr>
<tr>
<td>$h_b$, $h_e$</td>
<td>Impulse response of channel for users and eavesdropper respectively.</td>
</tr>
<tr>
<td>$X_b$, $X_e$</td>
<td>Signal transmitted by valid user and eavesdropper resp.</td>
</tr>
<tr>
<td>$N_0$, $N_e$</td>
<td>Additive white Gaussian noise with zero mean (AWGN).</td>
</tr>
<tr>
<td>$C_{ue}$, $C_{ue}$</td>
<td>Channel capacity of users and eavesdropper</td>
</tr>
<tr>
<td>$N_b$</td>
<td>Variance of AWGN with zero mean using Rayleigh Fading model.</td>
</tr>
<tr>
<td>SR</td>
<td>Secrecy rate</td>
</tr>
</tbody>
</table>
Table 2

<table>
<thead>
<tr>
<th>S. no.</th>
<th>Type of jammer</th>
<th>Detection</th>
<th>Prevention</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>RSS</td>
<td>CST</td>
</tr>
<tr>
<td>1.</td>
<td>Constant jammer</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>2.</td>
<td>Intermittent jammer</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>3.</td>
<td>Reactive Jammer</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>5.</td>
<td>Intelligent Jammer</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

The Table 2 summarizes the various types of jammers and their precautionary measures. From the perspective of 5G communication, all the nodes are in close proximity region due to increase in density of users. The presence of jammer at a particular location creates a consideration effect on the communicating nodes on a larger scale. If the jammer wants to disrupt the communication between A and B communicating parties but due to close association of nodes C and D. It will also disrupt the transmission between C and D or nearby nodes also. Any sort of noise added will hinder the transmission to a wider range. The metropolitan area will suffer from major loss as most of the transmission takes place through WLAN where basic element is the internet. Jammer will continuously transmit the radio signals resulting in DoS attack.

### 2.2.1. Types of jammers and their countermeasures (Zou et al., 2016)

#### 2.2.1.1. Constant jammer

It is a type of jammer in which the adversary continuously transmit the radio signal even the user is transmitting the data or not. However, this jammer suffers from high power deficiency or energy inefficiently as it continuously needs to transmit signal with high power all the time. The main aim of jammer is to interfere with the received signal quality. So when the legitimate user tries to sense the channel, he will always find the channel busy. For the detection of constant jammer, there is simple techniques and parameters which needs to monitor such as RSS, CST and PER. At the receiver end, the measured value of the signal strength or the energy is compared with the threshold value. If the compared value is greater than the threshold then this will assure the presence of jammer. The PER indicates the presence of jammer which usually has 0.1 default value and in abnormal case the value switches to 0.2 or more which leads to high PER. PER is defined as the ratio of number of incorrect packets received by total number of received packets,

\[
\text{PER (approx)} = \frac{\text{BER} \times N}{1} \tag{6}
\]

where BER is the Bit error rate probability and N is the number of bits in a packet.

The protection against the jamming attack is done by frequency hopping technique. It is a technique in which frequency of the carrier is changed either randomly or through a sequence. However, it is done through 2 methods by which it is done, 1) proactive frequency hopping and 2) reactive frequency hopping. In proactive method, the transmitter pseudo-randomly changes the carrier frequency without detecting the presence of jammer. In reactive method, firstly the presence of jammer is made and after that technique is implemented. The generation of pseudo-random sequence is done by cryptographic techniques which requires the sharing of secret keys for the transmission of data from source to destination.

#### 2.2.1.2. Intermittent jammer

The jamming signal is transmitted at a fixed interval of time by the attacker. It saves energy during the non-operational period as jammer transmits for a certain period of time and sleeps for the rest. For energy constraints jammer, this types proves useful as compared to constant jammer. The frequency hopping technique is used for the protection after the jammer presence is detected. Alternatively when the jammer gets activated, the legitimate node can switch to another channel for the transmission of data.

#### 2.2.1.3. Reactive jammer

The reactive only transmits the signal when the legitimate nodes gets activated. The reactive jammer is successful only when it is able to detect the status of legitimate node. The effective method of prevention from reactive jammer is by disrupting communication by making the legitimate node undiscoverable by the adversary. Using DSSS technique, the reactive jammer is unable to detect when the node is transmitting the data packets as it spread the signal to a larger bandwidth by lowering the PSD. The frequency hopping is effective when the hopping rate is same as to compare reaction time of the jammer.

The Table 2 summarizes the various types of jammers and their prevention mechanism.
to signal propagation and the advertisement of location should be taken care of.

The concept of popular scheme for detection in WLAN used for strange behavior of legitimate node is DOMINO. It can be implemented for MAC layer to detect the greedy behavior of nodes which is similar in case to jamming IDS. It consists of two test components: 1. Deviation estimation algorithm and 2. Anomaly detection algorithm. The final module called Decision Making component where the results from previous tests were combined and based on the results decision is made for the absence or presence of adversary.

For UDN in 5G, distributed IDS could be used as proposed for wireless network in Aime and Calandriello (2016). In case of densely populated network, there might be possibility that due to jamming attack the whole network could collapse. Each and every node in the network should monitor the ongoing network and note down the anomalous behavior if observed. This can be done by exchanging the lists among themselves. The devices which are critical in terms of power need to install IDS. The monitoring should be left to few nodes which are static and power issues are not present in them. Another idea is that we can deploy separate nodes for monitoring the network parameters and they should report to the central unit at a particular instance of time. For them sharing the information needs to be protected with cryptographic methods. The nodes which are mobile will have the least probability of considering it as a jammer. The installation of IDS should be application specific and depending upon the sensitivity of the information.

In the typical architecture of the UDN, they have utilized the properties of relay to a greater extent where one of the jamming node (or relay) acts as a barrier for the eavesdropper. But many times, the jammer needs to have the complete information about the CSI of the eavesdropper or the nodes which are affected by it on a large scale basis which involves complicated calculations and in many practical cases it does not result in plentiful task. In Complexity-Aware Relay Selection for 5G Large-Scale Secure Two-Way Relay Systems, they have designed low-complexity relay selection based on the amount of signals received for two way relaying with amplify-and-forward scheme such that when attacker tries to decode one signal the other one acts as a noise for it. So this way secrecy could be achieved.

2.2.3. Mathematical modeling for physical layer security (jamming)

As described earlier in the physical layer security, we need to have CSI of all the users like Alice, Bob and also of Eve. But the problem is with the estimation of channel state where only the information between Alice and Bob can be obtained. We cannot predict the channel nature of Eve completely. There is also another issue that the partial values of CSI is obtained for legitimate connection and they may be subjected to fading effects also.

The important analysis is the Shannon Information Theoretic Security for obtaining the secrecy capacity. The secrecy capacity is defined as the rate at which one node transmits the secret information to other.

1. For a discrete memory-less AWGN wiretap channel, the secrecy capacity is defined by

\[
SR = \max_{x} \{ C_M - C_W \} \text{ when } F[x^2] \leq P.
\]

where \( C_M \) and \( C_W \) are channel capacity of main and wiretap channel and is given by

\[
C_M = (1/2) \log(1 + S/N_M)
\]

\[
C_W = (1/2) \log(1 + S/N_W)
\]

The co-variance matrix needs to be designed for multiple antenna wiretap channel for achieving a good secrecy rate. Here the assumption is that all CSIs is known to Alice. Secrecy capacity of Gaussian Multi-antenna wiretap channel mode is

\[
SR = \max \{ \log \det(I_M + H_M C_M I_M) - \log \det(I_W + H_W C_W W) \}
\]

\[
C \geq 0 \text{ and } T(C) \leq P
\]

where \( I_M \) and \( I_W \) are identity matrix of additive Gaussian noise. \( H_M \) and \( H_W \) are CSI of main and wiretap channels respectively. \( C \) is the co-variance matrix. Eq. (10) describes the secrecy rate of multi-antenna wiretap channel where intermediate node is considered as shown in Fig. 3.

2. Partial CSI solution: As mentioned earlier, sometimes we do not have the perfect picture about the state of channel of Eve which is desired for calculating optimal wiretap coding. The \( H_E \) of the Eve is modeled based on the practical CSI as follows:

\[
H_E = \sqrt{KD} + n - \sqrt{KH}\hat{F}
\]

where \( K \) is constant and if \( K = 1 \) then Alice has perfect CSI and \( K = 0 \) indicates that the Alice has no information about CSI of Eve or Eve may be operating in sleep mode.

For \( 0 \leq K \leq 1 \), partial CSI information is present. \( \hat{F} \) and \( D \) is the indeterminate and determinant of the CSI statistics.

2.2.4. Challenges in physical layer security

This section addresses the issues that will be encountered when wireless security is implemented. In the previous sections we have discussed the security for massive MIMO and the jamming attacks and how we can overcome those problems. But still there are large number of issues still present which needs to take care of and we will be discussing many of them one by one.

1. It is already mentioned that for achieving high secrecy rate in a network, the CSIs of all nodes including the eavesdropper are required. But in practical scenario, this is not the case either we would have the partial information of the channel state or no idea of the eavesdropper when it is operating in sleep mode.

2. In many papers, the proposal for only one attack is present (Zou et al., 2016). In case of combination of two attacks or for distributed nature of attacking nodes, there is no such defending mechanisms present. Such methods needs to be implemented which will incorporate the joint incorporation of different types of attacks like eavesdropping with DoS. Considering the case where the CSI of the eavesdropper is unknown and also for the wiretap channel, it is of interest to plan such security protocol in such scenarios.

3. There are two types of eavesdroppers: Active and Passive. The active eavesdropper is effective when channels are highly uncorrelated between the attacker and the user. This means that adversary needs to align itself in such a position to become passive such that the channel is highly correlated between adversary and BS rather than between BS and User.

4. Another technique which could be used is the cross-layer security design. The traditional security algorithms introduces latency and computational complexity. The designing should be such that at each layer authentication scheme should be present. This method relies...
on all the layers. The deployment of different security methods at different layers increases the security level. Further, increase in level of security introduces the cost constraints and complexity which introduces the latency in the network. So the designing should be such that it should not effect the overall performance of the network with reduction in network overhead.

5. Due to tremendous growth of UEs in 5G and the introduction of new smart devices for multimedia applications led to increase in traffic substantially. For next generation, new wireless technologies are developed like massive MIMO and mm-wave. However, the need of security for the information is desired. The large number of antennas and use of high frequency band provide solution for the hungry of high data rate but all those benefits come at a cost. In massive MIMO, the increase in number of users give rise to serious issues of pilot contamination and power allocation. Such encryption and authentication mechanisms should be implemented which will compromise with the power constraints.

6. One of the main issues related to physical layer in heterogeneous network is the interference due to adjacent nodes where the presence of inter-cell interference cannot be avoided. For AN aided mechanism careful designing for transmission needs to be done in order to ensure safe delivery. So secure transmission is a major challenge in it.

2.3. Device to device security in 5G

D2D is a new technology in which two nodes communicate with each other without or less interference from the network. It operates either in standalone or network assisted D2D communication depending upon whether network is involved or not. There are certain issues which need to be solved for the D2D communication like power optimization, security, resource management. The four security attacks are defined in Alam et al. (2014): 1. eavesdropping, 2. impersonation attack, 3. attack on control data and traffic data. We will be discussing each one of them and prevention from these. Alam et al. (2014) have also specified the security requirements specifically for D2D pairs which could be beneficial during the deployment of UDN such that security architecture for the core/small Network could be used efficiently thus reducing deployment costs to the operators.

D2D is similar in working with the MANET but the operating areas are different like D2D works in licensed as well as unlicensed band depending upon whether it is in coverage area of small cell or not, whereas for MANET, it works in unlicensed band such that the problem of interference is a big thing (Wang and Yan, 2016). The security issues of MANET are different as surveyed in Djenouri et al. (2005). The origin of application area for D2D is the Bluetooth, WiFi-direct and Near-Field communication (NFC).

The attack scenarios in D2D are: 1. When D2D pairs are in coverage area of BS, 2. When the pair is outside of coverage such that signal strength is low. Thus, taking the help of relay and 3. When D2D nodes are out-of-coverage area of BS and they form ad-hoc network among themselves as shown in Fig. 4.

Another new technique of D2D pairs formation which is taken from wifi is wifi direct protocol. The operating principle of wifi direct is that the nodes form the group without any intervention from the owner group (OG) or BS (Mantas et al., 2015). However, the new protocol suffers from a lot of attacks possibilities due to flaw in its security designs and is equipped with wifi security setup using WPS. Shen et al. (2016) listed out some security challenges while integrating D2D pairs using WiFi direct which are: 1. Eavesdropping, 2. Impersonation, 3. Message Modification, 4. Man-in-middle and 5. Denial of service. The number of the attack is not limited to only the above mentioned types. However, in Shen et al. (2016) the key established is performed through the involvement of KDC (key distribution center) and PKI. The distribution is done on dynamic basis and is considered as a complex task. They have used Diffie-Hellman key algorithm for key exchange which is subjected to MITM Attack. Since a considerable number of vulnerabilities are encountered. So a short-authentication string based key agreement protocol is designed having reduced mutual authentication or less human involvement (Shen et al., 2016). These small applications are considered as a part of UDN scenario and any sort of attack encountered in it although on small scale can considered as a part of it. Recent work on constellation diagram has been done in Sun et al. (2016) related to D2D security. Such a scheme is proposed which helps in removing interference with the adjacent cells and thus achieving security. Or it can be said that interference free link establishment technique is proposed with inherit security embedded in it. The comparison between the SEP and SNR4B is done using superposition coding scheme, two-way overlay scheme and the proposed scheme with CSI-free and CSI-based rotation. Hence, they have concluded that with increase in SNR, SEP decreases with indicates the reduction in interference and simultaneously achieving secrecy rate (or security) as expected for the proposed model. Although another solution for protection D2D is either by encrypting the data between the nodes or authentication could be done at the BS side. Alternatively, by creating closed group access for the D2D communication the security can be maintained. But gives rise to yet another problem of impersonation attack in which attacker forges the identity of the client and tries to communicate or send packets on it behalf. The authors in Gandotra et al. (2016) have proposed the use of IP security for protecting the packets transferred between two nodes as the probability of getting attacked is considerably high for them. The authors in Liu et al. (2015) have proposed secure transmission for energy constraint D2D pairs using Power beacons deployed at various locations. The combination of energy harvesting along with secure transfer is introduced with the selection of best power beacon, Power beacon nearer to user etc. With the increase in the users, the considerable drop in value of secrecy outage probability is observed as increase in multi-user diversity gain (Mukherjee et al., 2014). Hence, causing increase in Secrecy Throughput.

Variety of new applications are added in the 5G network having increase in the number of users with the efforts of providing ease to the customers and they can communicate to a distant location without much hassle. One such type is related to medical applications which incorporated the concept of D2D data transfer. Now a days, we have seen many new things incorporated through the internet and any kind of medical assistance could be given to patients from a doctor at a distant location. Based on the reports or the information, examination or suggested solutions could be provided. Another aspect is that medical centers like small health centers, large hospitals etc have their backup present somewhere on the internet. All the information are stored already on the cloud or at the back end. Thus not requiring much file work for maintaining the patients record. This new application is introduced in the dense network environment of 5G providing flexibility to users. Some things comes at a cost and here the relation is in context to privacy or confidentiality of the user data. Any kind of changes in the person information lead to incorrect diagnostics and this can be very harmful as this results in the risk of patients health.

The authors in Zhang et al. (2016) have designed light-weight security scheme for M-health applications called LRSA. They have also proposed certificate-less protocol for generalized application which proves to be very effective in maintaining security using session key, and private key of physician. They have also compared the performance objectives with the existing schemes and it is observed that this new technology outnumbers existing proposed schemes. Most of the work is making efforts on maintaining authentication and confidentiality of the users as prevailing drawbacks in the D2D scenario where the affect of eavesdropper, sending fake messages, privacy violation etc are present. The possible solution to the attacks present in D2D communication is to provide protection to data transferred between UE and servers, servers to further core Network. All we need to provide is mutual authentication between users and network such that integrity is
provided to control as well as valid traffic data. But the key management and exchange is needed to be done very carefully without much involvement of air interface. Zhang et al. (2016) have proposed an algorithm to improve the secrecy rate of cellular users using D2D pairs which acts as a friendly jammers for them. Only one D2D pairs is able to reuse the Radio channel which simultaneously takes part in the transmission and side by side provides help during the uplink transmission for the UE. However, for multiple D2D pairs associated with a single channel they must compete among themselves who provides maximum benefit to the network in terms of performance. Such schemes gives the idea in a way how efficiently and in which assisted manner D2D pairs can provide potential benefit to the network for resource constraint devices and these things need to be explored in a better way.

2.3.1. Other issues with D2D pairs

With the introduction of device to device (D2D) communication, the task is to maintain the secrecy between the pair of devices. As the chances for overhearing the information by the attacker from the surrounding is very large. For devices which cannot handle high computation complexity for them alternatives need to be designed for providing security at the physical layer without much deterioration in their power consumption. One possibility could be the use of closed groups in which only a specified list of users have the access to form the device pairs (Yang et al., 2015). But this proves useful for a group of pairs and any list update need to configure the whole thing again. Second criteria is the open access groups which is limited to only one cell only but might be subjected to interference by the eavesdropper.

Another aspect of D2D communication is the deployment of relays which have the best transmitting capacity and geometry is selected for acting as an intermediate for the receiver device. Optimal selection of relays are required and investigation of untrustworthy relays are required in case of D2D relaying.

2.4. VANET security

The recent report from Cisco Visual Networking index showed that monthly global mobile data will be 30.6 exabytes by 2020 which consists of only 75% of video traffic (Eiza and Shi, 2016). Hence 5G acts as a new paradigm shift in order to meet these growing demand for new vehicle, devices etc.

Vehicular technology is an addition to new 5G technology with many significant researches done so far for the large scale deployment of it. But due to scalability, high mobility feature, latency and also the privacy issues make the deployment of vehicular network a tedious task. Many security issues need to taken care of like the authentication where high mobility users need to prove their identity fast. The problem of handover is also present. For the UDN, as the cell size shrinks to provide high data rate to users. The handover rate for high mobility user also increases and also the interference with the adjacent cells. Moreover, there arises yet another issue of near-far problem where every node is giving a good signal strength in its area. So the security constraints in VANET need to be taken care of because the presence of legitimate node could be misunderstood for rogue AP. The vehicular network is assumed to have D2D connection where the link is based on LOS path and is expected to less fading. Hence it proves as a real time application for future in mobile communication. Another data propagation present in VANET where the data is relayed to provide the best coverage area and hence subjected to many security issues. There are many recent work done so far in VANET security concern which are summarized in Table 3.

The network monitoring in the VANET is done by using IDS which will continuously monitor the network for any kind of abnormality observed in the network. The cluster based approach is followed which is based on the concept that in a network clusters are formed and out of each cluster the detection task is given to one node. It is always not the case that some outsider is compromising the security but there may be some cases where the attack is initiated inside the network called the misbehaving nodes. The transfer of data in a VANET is done in Ad-hoc manner where the data transmitted from one node either have to go through one hop or multiple hops ultimately reaching to the desired location.

The Fig. 5 represents the basic scenario of vehicular technology where the road is having many access points deployment on road side. Whenever the data is transmitted from source it establishes a D2D link with the adjoining vehicles or with the AP. TA is connected with the DMV and LEA such that in case of any emergency situation action could be taken immediately. The adversary can generate the attack against small cells, vehicles, DMV or LEA and hence enable two types of attack scenarios either internal or external. The external adversary can monitor the network and capture the packets or learn about their locations and the information contained in the packets. For internal adversary, the nodes are compromised and can be forced to do abnormal activities which is controlled by some outsider similar in case with botnet attack. Here TA can be assumed to monitor a particular region and all the TAs are inter-linked with each other.

The authors in Zhang et al. (2015) proposed the secure data sharing between any pair of D2D devices in which collaborative approach is followed where Public key based digital signature with mutual authentication mechanism is used hence guaranteeing authentication, integrity, non-repudiation etc.

Humans are assumed to be most careless and risky drivers as most
of the faults on driving and accidents are caused by human negligence. Thus affecting a large number of people resulting in deaths and major accidents. VANET proves to be promising technology in the present scenario and many new extensions are proposed for increasing the performance of this immature technologies. Gerla et al. (2014) One of them is the Driver-less cars or the driver-assisted cars equipped with modern navigation system, advanced safety features featuring high quality of lifestyle. A novel technique of message authentication is proposed in Joseph Abueh and Liu (2016) making VANET resistant to DoS especially designed for Driverless cars and companies manufacturing them are Google, TESLA, Audi etc. However, the author has suggested the use of digital signature for encrypting messages using with either PKI or group messages. For the vehicle which is far away from the authentication center for them multi-hop authentication schemes should be proposed where the messages are hopped through neighboring nodes. However, this scheme needs a lot of reliability in the sense that the critical information is routed through nodes which also need to prove their identiﬁcation. Bariah et al. (2015) have also explained the vulnerabilities present in AUV and basic cars which are suspected to many attacks by the adversary like DDoS by disabling the steering system of cars or brakes system. These attacks are more crucial in case of AUV due to the lack of driver presence. However, the designing of cars should be managed very carefully. In case the cars are suspected of any malicious behavior, the OBUs should be given authority to manage the control.

Liu et al. (2015) have listed out some major security attacks keeping in mind Security issues as follows: Snooping Attack, Traffic Analysis, Data modiﬁcation, Replay attack, Masquerading, GPS spoofing, jamming, Black Hole, Timing attack, Illusion Attack, Bogus information etc. An ASPE scheme is proposed in Huang and Verma (2009) which Incorporated data control, dynamic key generation, security policy for dynamic environment in VANET. Also, the proposed framework is efﬁcient in coping up with various attacks like simple attack, bad-mouth attack and zig-zag attack. Depends on signature and online/oﬄine scheme for identiﬁcation purpose of road-side units and vehicles also. Efficient in coping up with various attacks like simple attack, bad-mouth attack and zig-zag attack. ART mechanism is proposed where the data trust and node trust factor of the data is veriﬁed on the basis of data collected and sensed from different moving vehicles.

<table>
<thead>
<tr>
<th>S. No.</th>
<th>Year</th>
<th>Author(s)</th>
<th>Contribution</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.</td>
<td>2011</td>
<td>Wei Hu et al. (2011)</td>
<td>Proposed ATCS scheme which provides efficient combination of group based threshold signature and anonymous signature scheme resulting in signature overhead.</td>
</tr>
<tr>
<td>3.</td>
<td>2013</td>
<td>Barba et al. (2013)</td>
<td>Proposed crowds protocol for VANET users which will report in case of traffic violation irrespective of interference of infrastructure such that not to comprise with the identity of reporting user.</td>
</tr>
<tr>
<td>4.</td>
<td>2014</td>
<td>Wahab et al. (2014)</td>
<td>Two phase model has been proposed to detect misbehaving nodes during or after cluster formation using cooperative watchdog model based on Dempster-shafer approach. Thus maintaining QoS, reduced false negatives and probability if detection.</td>
</tr>
<tr>
<td>5.</td>
<td>2014</td>
<td>Alam et al. (2014)</td>
<td>Three Types of use cases and D2D scenarios described depending upon absence and presence of D2D user which is application specific and also deﬁned different types of direct radio link attacks in it.</td>
</tr>
<tr>
<td>6.</td>
<td>2015</td>
<td>Li et al. (2013)</td>
<td>Proposed an ACNP framework for VANET based on public key cryptography for generating pseudonym identiﬁers instead of vehicle IDS.</td>
</tr>
<tr>
<td>7.</td>
<td>2015</td>
<td>Li and Song (2015)</td>
<td>ART mechanism is proposed where the data trust and node trust factor of the data is veriﬁed on the basis of data collected and sensed from diﬀerent moving vehicles.</td>
</tr>
<tr>
<td>8.</td>
<td>2016</td>
<td>Eiza et al. (2014)</td>
<td>Proposed novel scheme for QoS improvement and secure transmission using Ant colony optimization technique with the aim to provide the best path for transfer of vehicle data using robust routing protocol.</td>
</tr>
<tr>
<td>9.</td>
<td>2016</td>
<td>Eiza et al. (2016)</td>
<td>Proposed system model for real-time video reporting service in case of emergencies or misbehaving owners so that any kind of assistance could be provided immediately.</td>
</tr>
<tr>
<td>10.</td>
<td>2016</td>
<td>Wahaba et al. (2016)</td>
<td>Proposed CEAP deals with the users having high mobile nature (VANET). The design is based on QoS-OLSR protocol. Thus improving detection ratio, decreased false positive rates with improved packet delivery ratio.</td>
</tr>
</tbody>
</table>

2.5. Internet of things (IoT) security

The Internet of Things acts as new emerging technology in the 5G architecture which includes the involvement of sensors for variety of applications with high computational capabilities. The architecture of 5G which is very diverse characteristic and incorporates a variety of heterogeneous network including IoT also. It includes avast area of application like home appliances, industrial automation, smart objects, hospitals etc where small sensors are present to be taken care of numerous number of things. All the data are transferred through...
internet or a global platform. However, IoTs suffers from major drawbacks which are listed as follows: 1. Many applications which are covered by IoTs critically depends on the low latency requirements of few milliseconds which is difficult for cloud services to provide to users. 2. As the number of devices increases exponentially in the coming wireless communication architecture and each device has many controlling devices connected through internet hence generating larger data than expected in the coming years including video data and voice data mainly. This gives rise to high network bandwidth requirements out of which 90% of the data are handled within the network (Chiang and Zhang, 2016), 3. Protecting the devices which do not have sufficient resources in terms of power requirement for them managing their own security is a difficult task. For sensors, actuators etc. suffer from battery drainage problem for them such mechanism should be present having either distributed or centralized characteristics., 4. there are many devices connected through the network needs to be updated on a periodic basis and managing their security credential on a regular intervals is a difficult task to perform., 5. Many new applications which are added in the 5G architecture deals with health monitoring systems in which data is collected from sensors including log data and status messages. The devices lacking in security features can be used to send the false messages and information. Many times adversary try to leave the devices in non-working conditions i.e physical hampering is done and the working of devices well intact.

2.5.1. Security challenges in IoT

Here, in this section we will be concentrating more on security issues related to IoT devices in details. The basic architecture of IoT consists from two main protocols namely: a) 6LoWPAN and b) CoAP (Nia and Jha, 2016). 6LoWPAN is a combination of both IPv6 and IEEE 802.15.4 used for embedded nodes having only restricted set of protocols. Whereas CoAP is a special protocol designed to provide services to only small low power sensors (Nia and Jha, 2016). However this LoWPAN is used for short radio range, Low Direct Range, Low power and Low cost communication and features FFD and RFD devices. IoT enabled with LoWPAN supports star topology where all the smart devices are connected to a central coordinator rather it transfers information to a single entity. Another is Mesh topology where every node is connected to one another (Table 4).

In this topology, the information exchange is done with the help of inter mediator i.e through gateway. IoT is based on IP based network where a large amount of traffic is generated to billions of devices which would be crossing a threshold level of 50 billions by 2020. Certainly it would be very difficult to manage such wide connections and the attack arising from the collection of various IP devices is difficult to handle. In order to reliability of data transferred, various security challenges are faced by the researchers and the providing protection mechanism against them and we will be addressing such of the attacks one by one in this section. IP spoofing attack, the adversary tries to capture the IP packets generated from source and the senders address is modified with spoofed/forged IP address. Hence it results in social attack and thus creating damage to network on a larger scale.

Despite the attacks mentioned in Fig. 6 there are other possibilities like Interference based attack where the adjacent nodes or cell region creates disturbances during transmission source node to destination node. So interference management is a critical issue particularly for UDN especially for IoT devices where the for every small computing device is implanted. The authors in Komninos et al. (2014) have presented the vulnerabilities in smart homes and grids. They have categorized attacks based on the region and also listed out the countermeasures. The authors in Granjal et al. (2015) have also presented survey on security threats present in existing protocol of IoT. Another very famous area in IoT is the Medical Heath Monitoring where small sensors are used for monitoring the health of patients. Such a large usage of sensors for monitoring purpose raises an important question of its effect on patients health. Another concern in 5G deployment scenario is the handling such a large integration of devices all together. We can also say that how to collaborate such greater density so that they all can work efficiently without much hassle i.e Management Issue. Before the addition of new user/device, we need to first check its protocol stack such that the proposed security mechanism is compatible with existing architecture.

IoT architecture is essentially based on purely IP addresses where every device require its own IP address. There might be chances that with heavy load on the network in UDN, there will be loss of unique identity or in other terms there might be possibility of IP interference which results in page expires or IP conflict which needs to be taken care of before such network is merged with the existing network.

2.5.2. Protection/security mechanisms present in IoTs

IoTs proves as a new emerging technology for a number of smart services ranging from smart computing to health services and hence required potentially high protection from the attacker and a good quality of services. Considering the case of patient admitted to hospital wearing smart devices for getting the status about its health issues he/she is facing and any transfer of information through insecure medium could result in the manipulation of critically important data where the health of patient is at stake. One such traditional scheme for the

Table 4

<table>
<thead>
<tr>
<th>IoT challenges</th>
<th>How the issues can be resolved</th>
</tr>
</thead>
</table>
| Latency constraints    | For time sensitive applications or in real time processing of data analysis, this parameter plays a critical role.  
|                        | The issue can be resolved with the help of installing mediators both for non-IP or IP enabled smart devices (Giuliano et al., 2016). Another technique could be the use of Fog (Chiang and Zhang, 2016) for time-sensitive applications. |
| Bandwidth requirements  | Storing the data locally rather than sending it to cloud could help to reduce load on cloud servers.  
|                        | Creating one network for non-IP IoT devices and mediator assigns the address to its own group just like NAT.  
|                        | The important traffic is filtered out by some agent and passed on to cloud with the increase in the amount of traffic.  
|                        | Distributed architecture of IoT devices helps to cope up with need for high bandwidth requirements. |
| Resource Constraints Devices | Devices which are lacking in resources for them the computational load related with either to security or any other functions is performed by any other devices and also their periodic health monitoring of the devices could be easily performed |
| Security Challenges    | Problem of authentication can be solved with the use of biometrics for feature extraction with or without passwords (Hossain et al., 2016).  
|                        | “Cognitive Security”where authentication of user is based on the knowledge and pattern pertaining to a user which has received validation through leaning.  
|                        | IDS can be integrated with Cognitive Security for better performance in area of device security.  
|                        | Incorporation of TLS with onion routing scheme for providing confidentiality and integrity.  
|                        | Mediator (or gateway) acts a representative to other part of network for non-IP devices. The data transfer between gateway and outside network can encrypted. |
protection of IoT devices is the adoption of 2-factor authentication scheme based on passwords for providing user authentication (Chakib, 2014). The main drawback in the 2F-A is that password present in it can be changed/modified. Thus making it insecure or inconvenient to use.

Another new technology called Fog which acts a replacement for cloud business and hence provides better connectivity and faster computation towards the end users rather than providing the data storage at the remote locations.the nature of fog is distributed covering a comparatively larger coverage area than the cloud. The controlling function of the fog is done through small companies and merely by any technical operators. As compared to cloud any challenges which are addressed in the introductory section of IoT is resolved through fog. The new technology proposed in Hossain et al. (2016) helps to overcome a number of limitations including security challenges like it acts as a proxy for many devices which are lacking in terms of resources and helps them to mange their security updates. It also takes care of the status of surrounding objects and based on the information collected protection is provided. There is still one issue which need to be taken care of before installing fog is that while integrating devices with fog technology, the data transferred needs to be encrypted and well managed. It is subjected to more attacks than the centralized systems.

The authors in Xu et al. (2016) have focused on secure transmissions through relay in IoT networks exposed to eavesdroppers without any information about its location and strength. They have used random-and-forward relay strategy for multihop secure relay transmission where it is observed that the secrecy rate achieves high value for direct communication but gradually decreases with increase in the hop count. Also with consideration increase in value of SNR(dB), the average secrecy throughput also increases for single antenna and single relay transmission (Xu et al., 2016). Generally, one hop transmission is safe Le message recovery is difficult to perform. For Low-end sensors in IoT like source and destinations for them AN is not an appropriate choice for data transmission as the power consumed for generating the noise will be more thus effecting the performance of devices to a greater extend and also causing huge amount of interference to neighboring nodes. In such cases, appropriate beamforming technique is a feasible choice (Du et al., 2007).

Cao et al. (2014) Bio-metrics identification can act as an alternative authentication mechanism for 5G networks serving a large amount of application area from D2D to massive MIMO compared to tradition way of authenticating the data by Hashing schemes like HMAC etc. It serves as efficient way and provides secure services in a number of areas through fingerprint scan, iris scan or face recognition. For incorporating such a drastic change in the scheme like using above mentioned methods to authenticate the messages instead of passwords etc, we need to hold a large amount of database for group of people where one information is not sufficient because if one fails other can serve as a backup for it. The authentication scheme based on bio-metrics have a limitation of computing the resources and storage as these features are very difficult to process which involves the processing of multimedia signals which leads to slow identification of the person while logging off based on the information retrieved. For multimedia applications where low delay is required and fast response from the system is expected. So it is great challenge to provide subscribers with such a controlled environment where everything would result in a perfect scenario.

The new authentication mechanism which could be implemented in IoT devices is biometrics based scheme using fingerprinting scan, iris scan etc along with password. Hossain et al. (2016) used face biometrics scheme for opening of smart phones or making any financial transactions. The sensors captures the face image and try to retrieve the traits of the person. The information collected through the sensors is sent to database which already contains the information of the users and it is matched against it. The FBI, Windows 10, Apple, Samsung etc is giving stress on biometrics based authentication scheme as a basis for security alternative. Some companies have also announced the combination of biological traits with traditional scheme.however, this methodology suffers from complexity while implementation. But this kind of implementation is still in testing phase and requires a lot of extensive research, so that new research issues can be tackled in it. The detailed survey on the security issues related to cloud have been presented in Fernandes et al. (2014).

Some smart devices and IoT devices (e.g. Sensors, health-care monitoring devices etc.) try to store their data on public clouds of Amazon, Google, IBM etc. which are prone to security threats. However, in this implementation of biometrics based scheme which facilitates the installation of new ubiquitous environment but this new authentication based scheme fails in providing end-to-end security among smart devices and sensors. Once the adversary is able to get the information about the traits of the person, he/she cannot implement attack and try to hijack the session by dynamically generating the key because as adversary is unable to pass the dynamic process by generating data based on real-time analysis. Hence, it provides protection against replay attack and masqueraders, thus providing the users with confidentiality and integrity.

Another application of IoT for providing secure communication is the use of RFID which integrates multiple application. Fan et al. (2015) has proposed secure scheme for RFID multiple application and single application RFID tag and hence this scheme proves to be useful than the conventional scheme of encryption and authentication scheme which further limits the performance of RFID tags having low cost. For each RFID tag the period of its validity is set and corresponding list of applications integrated in it. Once the time period or lifetime of tag gets over the tag application is canceled.

IoT applications is built to connect million of devices with each other and thus generating large amount of data at the edge level or
directly from the environment as to act as a interface between the real world and real world. However, for the protection of devices connected through internet we need to have the information of the state of the channel to achieve high secrecy rate which is estimated in terms of secrecy outage probability. But in practical scenarios getting CSI information is a difficult task. Chen et al. (2016) have introduced smart channel sounder for IoT devices in a wireless channel which is used to predict the nature of the channel based on the values of m parameters using Nakagami-m fading model. However, the conventional scheme fails to achieve any such information of the state. Chen et al. (2016) The PDF is defined as

\[
P(r) = \frac{2}{\Gamma(\alpha)} \left( \frac{p}{\alpha} \right)^{\frac{\alpha}{2}} e^{-\frac{p}{\alpha} r^{2}} \phi, \quad r \geq 0
\]  

(12)

In case of two hop transmission where relays are used and acts as a intermediate node for the transmission of data, in such scenario using encryption process becomes a tedious task as the end nodes are having distributed architecture and they are also lagging in terms of computing capability. So to achieve a good desirable level of secrecy rate or performance, physical layer security serves as the best alternative in this regards. Zhang et al. (2015) have analyzed the secrecy outage probability for M-colluding eavesdroppers such that they can combine their resources to decode the message. Based on the classical probability theory, Secrecy outage probability is defined as

\[
P_{\text{sec}} = \Pr \{ C_{E} < R_{1} - R_{2} \} \]

(13)

\[
P_{\text{out}} = 1 - P_{\text{sec}} = 1 - \Pr \{ C_{E} < R_{1} - R_{2} \} \Pr \{ C_{E} < R_{1} - R_{1} \}
\]

(14)

where \( R_{1}, R_{2} \) are the rate of code transmissions for user 1 and user 2 respectively.

For M users allowed to access the network in round-robin fashion is defined as

\[
P_{\text{out}}^M = \frac{1}{M} \sum_{i=1}^{M} P_{\text{sec},i}
\]

(15)

On further solving the above expression, we get

\[
= \exp \left\{ -\lambda_{s} \left[ \frac{p_{1}^{2} d_{1}^{2} - 2 R_{1}^{2}}{1 + p_{1}^{2} d_{1}^{2} - 2 R_{1}^{2}} \right] \right\}
\]

where \( p_{1}, p_{2} \) are the transmitted SNR at Source and Relay respectively. \( R_{i} \) is the Rate at which confidential messages are sent by the source.

Description about the notations are summarized in Table 5.

### Table 5

<table>
<thead>
<tr>
<th>S. no.</th>
<th>Notation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>( \alpha )</td>
<td>Inverse of path loss component</td>
</tr>
<tr>
<td>2</td>
<td>( P_{\text{sec}} )</td>
<td>Secrecy outage probability for entire transmission (M users)</td>
</tr>
<tr>
<td>3</td>
<td>( \xi )</td>
<td>Capacity of eavesdropper channel</td>
</tr>
<tr>
<td>4</td>
<td>( \lambda = 2 \Pi_{1} )</td>
<td>Polar coordinates for probability functions in PPP</td>
</tr>
<tr>
<td>5</td>
<td>( \beta )</td>
<td>Path loss component</td>
</tr>
<tr>
<td>6</td>
<td>( d_{i} )</td>
<td>Distance between two communicating nodes</td>
</tr>
<tr>
<td>7</td>
<td>( P_{\text{out}} )</td>
<td>Probability for secure transmission through relay</td>
</tr>
<tr>
<td>8</td>
<td>( h_{i} )</td>
<td>Small scale fading component having symmetrical Gaussian distribution with zero mean and unit variance</td>
</tr>
<tr>
<td>9</td>
<td>( \lambda_{e} )</td>
<td>Eavesdropper density modeled for homogeneous PPP</td>
</tr>
</tbody>
</table>

The Fig. 7 showed the possible security layered architecture of IoT. Whereas Fig. 8 depicts the system model for secrecy rate in the presence of relay node.

### 2.6. Security using energy harvesting technique

Energy harvesting is a powerful source of energy for providing long lifetime to energy constrained devices and replacements of devices. RF signals carry both information and energy which is very difficult for receiver to process both the things simultaneously. The simultaneous processing of signals for energy harvesting and information is performed in relays where source transmits the information to relays which in turn processes the RF signal for further movement of information to destination. Cooperative-relay scheme have been studied in Krikidis et al. (2009) for evaluating the performance of physical layer security in the presence of eavesdropper, who tries to intercept the signals transmitted by the source and relay. In the presence of eavesdropper, the secure communication can be provided between source and destination with the deployments of multiple energy-harvesting relays having multiple antennas. However, this scheme works for data transmission using untrusted relays in the presence of eavesdropper. Kalamkar and Banerjee (2016) The author evaluated the positive secrecy rate for information transfer between source and destination via untrusted relay using PS and TS policy separately on the received RF signal during the processing of information. The relay is enabled with energy harvesting algorithm which gets activated whenever the received signal power by the source drops below a required threshold \( t_{r} \) and simultaneously getting jamming signal from the destination. They have also analytically proved the expression for secrecy outage probability and Ergodic secrecy rate defined as (Kalamkar and Banerjee, 2016)

\[
P_{\text{out}} = \Pr \{ I_{\text{sec}} < I_{0} \}
\]

(17)

where \( I_{\text{sec}} \) is the instantaneous secrecy rate and \( SNR_{0} \) and \( SNR_{E} \) are the signal to noise ratio at destination and relay node respectively.

### 2.7. Security in Spectrum Shared Networks

Many organization have conducted studies such that the spectrum should be utilized to its maximum potential. Hence, to satisfy the growing demands of spectrum as new technologies are merging with the existing architecture day by day. An innovative technique is adopted which gives authority to the stakeholders to share their spectrum. The nature of different wireless networks is heterogeneous and each having its own spectrum requirements and performance criteria. Thus FCC made this spectrum sharing a legal task which could be performed very easily on lease basis for the duration assigned for the license (FCC 04-16, 2004). D2D pairs also share the same resources or frequencies as used by the single user. Hence, utilizing the spectrum in a more efficient way. Such that same frequencies can be used again and again. Although, it could also lead to interference with the adjacent nodes if they are sharing the same frequency bands. There are two method through which spectrum sharing is enabled: 1) through spectrum sensing in which either the nodes senses the medium in standalone mode or cooperative mode, and 2) connection enabled through Geolocation database. Database contains all the information about the spectrum sharing environment and the Secondary User first establishes connection with database before getting access to the spectrum. The general architecture for Spectrum Shared Network is presented in Fig. 9.

The SU can have possible and secured performance if no interference through the PU is promised. The access to the unlicensed...
spectrogram is either provided on yearly basis or annual basis. However, SU can also switch to another spectrum band if the connection request is rejected. The SU connects to the unused such that it would not affect with the working of primary users. Also the resources available to PU is sufficient such that it can further grant access to PU. Such auction of the spectrum to PU or by the PU’s need to be taken care otherwise it could result in potential security breaches and all the efforts taken to set up most efficient spectrum utilization goes in vain. In Fig. 10, the list of all the possible Security issues present with the spectrum sharing have been listed down. However, the attacks are not limited to the attacks mentioned below. As we have only summarized the major area of attacks with their common regions of possibilities. Physical layer deal with the transfer of information through the medium and the electrical components responsible for generating the pulses based on the information received from the above layers. Such that it can be

Fig. 7. Possible security region in layered architecture of IoT.

Fig. 8. System model for two-hop communication.

Fig. 9. General architecture for spectrum sharing.
subjected to interference from the adversary side whose aim is to get the relevant information. However, the adversary can send false reports to the SU’s who tries to establish connection with PU by sensing the medium such that no PU exists or the attacker can send information about the geographic location on behalf of SU. Attacker also tries to compromise with the information that is being shared by the incumbents. For the Geolocation database, the SU tries to send information to it as mentioned earlier which could also lead to location leakage threat. The best way remove the interference affect by the adversary is mixing noise in the information that is being transferred through source. Using RF fingerprinting or EM signal identification information send through mobile devices for the authentication of SU also solves the considerable level of security problem as the fingerprints by the user is a unique feature. In the same, some bits are sent along with the message for the identification of the user. Abdelhadi et al. (2015) Authors have proposed MTSSA algorithm for securing spectrum shared networks for multi-tier wireless systems to avoid fraud bids using Paillier cryptosystem. For more details about the attacks in various categories refer to Liu et al. (2015).

3. Ultra-dense network

Due to immense growth in the number of users from 3G onward. There is a utmost requirement for increasing the number of basestations in the coverage area. With the deployment of more base stations, the cost constraints also has an impact on the telecommunication sector. The concept of ultra dense network arises with increase in the density of users. The idea of enhancing the capacity can be achieved by increasing the spectrum efficiency (bits per second) using more efficient modulation schemes and channel coding techniques, increasing the spectrum bandwidth or reducing the cell size (Wang et al., 2014). It is concluded that by increasing the amount of access points in a coverage area of a macro-cell, the system capacity could be increased efficiently (Wang et al., 2014). The concept of small cells in LTE deployed in the coverage area of macro-cells results in the formation of heterogeneous networks (HetNet) to increase capacity. The main motive of discussing previous topics is that in some way or the other those technologies will be related to UDN architecture. In this section only, we have proposed the security architecture.

Unlike conventional cellular architecture where users only contacts the base station which further transfers to Base station managers for processing but in ultra dense network due to densification in the users, small scale integration has started with includes the incorporation of femtocells, Picocells, micro-cell or any hotspot deployment. The traffic of these small base stations will be forwarded to macro cell base station using back-haul links and these macro BS will forward the data to core network either through optical links, broadband internet. The area of coverage of micro cells will be overlapping with the macro-cells.

In comparison to macro-cell BS’s, the micro cells can provide with high data rates, lower latency. The handover process is controlled by both the micro and macro-cell managers but the procedure is typical as the fast moving user applications there is a great amount and frequent handover required. This adds an overhead where the need for handover is fast. To overcome this issue, all the management data to control the handover among users and micro-cells are done by macro-cells and only the data transmission is managed by micro-cells (Ge et al., 2016). The authors in Ge et al. (2016) proposed an architecture based on the distributed architecture having one gateway or multiple gateways is deployed in the macro-cells having installed the massive MIMO millimeter wave antennas for receiving and transmitting the signals of backhaul traffic. Through millimeter wave propagation traffic is sent from one micro-cell to another which further transmits all the backhaul traffic of small cells to macro-cell using multihops links. Ultra-dense network is an integration of both small cells and macro-cells.

The general architecture of UDN consist of Picocells, femtocells, consisting of Hotspots, relays and, macrocell. The applications covered by a typical UDN scenarios in 5G networks are hospitals, college campuses, railway station, airports, shopping malls, stadium, metro stations and so on. There might be cases where the population is very high. Those regions will be requiring large amount of cells coverage whereas for rural areas, the cell coverage area will be less. In Table 6, we have summarized different types of cells and security issues encountered in it.

3.1. Challenges with ultra dense network

The UDN suffers from major issues: interference, mobility, power consumption and backhaul (Gotsis, 2016). In the interference management, the mobile users which are the boundary of cell coverage suffers the maximum interference with the adjacent cells as the reduction in cell coverage area. Also, ultra-dense network consisting of Het-Net suffers the maximum interference than homogeneous cells. The cells in UDN has the high data rate due to small coverage area and it serves only few users with the
that mobility is very large. This give rise to sudden arrival and departure of users (Gotsis, 2016). Due to small cell configuration, it is expected that the handover process is too frequent. Handover procedure suffers from complexity for high mobility users. At the boundary of macro-cells, only the maintenance of control and data signals could be done because of lack of data rate. It is expected that throughput variations would be prominent during the handover process.

The backhaul link transmits the data from macro-cell to the core network which could be done either by the use of optical fiber or microwave link. The deployment of fixed backhaul (optical fiber) has a very high cost but with higher bandwidth benefit. It is difficult to reach some sites (Gotsis et al., 2016). Alternative to this is the micro-wave link, but it requires LOS communication. It also requires an additional equipment and spectrum license. Gotsis et al. (2016) It is suggested to use self-backhaul technique to resolve the issue. The green communication is stressed upon for low power consumption which leads to high energy efficiency. The maximum energy is wasted to keep the radio frequency unit active and sending control signals. During the deployment of femtocells, the desire of users low complex and low power is the utmost requirement still prevailing in UDN also. Such low complexity approach require an extra synchronizing scheme for the information exchange. Another requirement is the resource management covering a larger area using joint optimization technique also creates problem while the UDN are established (Zanella et al., 2014). The management of security related spectrum shared and power allocation along with the presence of additional noises creates a challenging task for the researchers (Zanella et al., 2014). It further raises and issue of complexity in the topology of UDN architecture and thus creating interference related issues within the cell or with the adjacent cell. With the increase in user density (or high QoS) would be requiring a proper balancing between complexity of the systems and security (Zanella et al., 2014) (Table 7).

3.2. Architecture of UDN

The basic architecture of 5G includes from core and management system to protocol layering. As of now, the basic definition of 5G has not reached a proper standardization in 3GPP. But there could be more scope for cloud and IoT technologies. The structure of mobile communication has reached from large cell integration to an idea of small cell deployment covering not only data and voice call across the world but connecting millions of people. It also includes hospital data in which data about patients health is all available online.

In Fig. 12, the general architecture of ultra-dense network is proposed. The area of macro-cell is divided into small-cells. Those small cells may contain Picocells, femtocells, academic area or any other office building etc. UDN concept also covers area like airport or railway station where the number of passengers are very large. These applications require indoor and outdoor deployment of seamless coverage and capacity. By 2025 or 2030, UDN will be covering urban indoor and outdoor area with edge rates of 100 Mbps to everyone in small cells (Peng et al., 2016).

All the access points within a cell are connected through internet which in turn will be directing the data to base station. Similarly, for small cell base stations, they form a direct millimeter wave link with the base station. The macro-cell base station is equipped with Massive MIMO having multiple transmitting and receiving antennas. In a typical scenario of UDN, it is expected that the value of throughput for mobile nodes present at the edge of cell have less value. Also, they have a common coverage area with the adjacent cell.

3.3. Road ahead of ultra-dense

Road Beyond Ultra-Dense is expected to have a large density of Access points practically 0.01–1 Active users/Base stations but in actual deployment scenarios is feasible for only indoor applications as the cost constraints is a major concern in this regards as suggested in Jens (2017). only suggested feasible thing to balance between technical issues and economic parameter is that if indoor users acts as a helper or serves the indoor users of the operator. As the major issue in dense deployment is the management of backhaul traffic and interference as cell coverage shrinks and each AP has a high SNR. As shown in Fig. 11, with increase in AP density Data Rate achieves a saturated value. Cost increases drastically with increase in Spectral Efficiency. The work has been taken from Jens (2017) and the results are merged.

3.4. Possible attacks on UDN

With the densification in 5G networks, the amount of traffic also increases. The users expect that the data transferred should maintain the confidentiality and integrity. Any violation in this regards is intolerable. This raises an important question about security of the network or for the mobile users. The ultra-dense network architecture could results in many possible security attacks which are follows (Fig. 12):

3.4.1. Relay-based attack

The relay is present in 5G network of small cell deployment on large scale basis. The users which are present at the boundaries of the SCA will transfer the information through relay. Basically, it covers the users which are located in the dead zones where the scope of signal reception is almost negligible. As a result, the users at the boundaries will be receiving more signal strength from the relay than the base station. However, the information transferred with this intermediate helper is done either through direct transfer of data or first by storing then further transferred to destination. Relay is a small and inexpensive device and there might be possibility that by any means intruder

Table 6: Different types of small cells and their security issues.

<table>
<thead>
<tr>
<th>Type of cell</th>
<th>Deployment region</th>
<th>Coverage</th>
<th>Power requirement</th>
<th>Access scenario</th>
<th>Security issues</th>
</tr>
</thead>
<tbody>
<tr>
<td>Picocells</td>
<td>Hotspots (indoor/outdoor)</td>
<td>Up to 100 m</td>
<td>≤ 100 mW (indoor traffic)</td>
<td>Open</td>
<td>Physical damage, Denial of service (DoS), Traffic monitoring</td>
</tr>
<tr>
<td>Femtocells</td>
<td>Installed to improve coverage area and capacity (especially residential area)</td>
<td>Between 10 and 30 m</td>
<td>≤ 100 mW (outdoor traffic)</td>
<td>Open/Closed/Hybrid approach</td>
<td>User privacy, Denial of Service, Service theft and Fraud, False location attack</td>
</tr>
<tr>
<td>Relays</td>
<td>Cell boundaries or load shedding purpose</td>
<td>Up to 100 m</td>
<td>Same as Picocells</td>
<td>Open</td>
<td>As described in coming section</td>
</tr>
</tbody>
</table>
tries to acquire the control over it. By controlling the relay, intruder will get the control over all the devices connected through it. It will try to exploit the features of relay and try to get the benefit out of it. Instruder can also change the MAC address. Thus making it unavaiable to the network or it could install malicious software to create the mobile botnet attack for remotely controlling the users of the network. Relay is an extension of macro-cell. The backhaul link of relay i.e microwave link have the susceptibility of getting attacked in which all the backhaul traffic is directed to the intruder chosen location. Relay will always be present at the boundary of cell which is shown in Fig. 13. The attacker present nearby to the relay will control and try to change the path of data transfer. But the end to which this attack causes damage depends on the overlapping regions of different types of cell.

Table 8 summarizes the various types of possible attacks in UDN with their possible solutions in descriptiver manner.

It is felt that number of picocells deployment will be more as compared to other types of cells and hence they can be subjects to in numerous number of threats.

3.4.2. Rogue access point

Another definition of ultra-dense network is where number of access point will be more than the users or we can say that in ultra-dense network one user will be served by only one access point ideally (Kamel et al., 2016). The users under one AP will be very less generally less than four. Not only user density increases but also AP deployment increases many folds. It gives rise to security threat because the base station is not knowing about the information of the APs. There could be chance that out of hundred or thousand AP, few are controlled or they are malicious and their aim is to disturb the ongoing network. This type of attack is only confined to small cell area (SCAs). The challenging issue in SCA due to high density is the interference problem either with the adjacent cell or within the same cell which give rise to security breach. Intruder will try to intervene with receiving signal rather it tries to transmit more power than the valid AP. The nearby users establish connection with rogue AP. Another, probability is that the malicious AP tries to prove its identity of valid AP. The effect of rogue AP attack become more prominent and hazardous when the receiving nodes are draining of power or they are experiencing more interference from the adjacent cell due to extreme level of densification within a macrocell. However, the level of dense network should have an limit such that it would not affect the network performance. Hence, providing the opportunity to the attacker to exploit the resources. Once the users are under the control of attacker. He/she can use them for his own benefit by extracting the user-names, passwords or credit card numbers resulting in another of attack i.e. access point phishing. In Fig. 14, the rogue based attack under dense deployments are presented.

3.4.3. Authentication based attack

In the basic architecture of 5G, we are assuming it to be more denser than 4G network having high mobility of users. It is also assumed that within large cell, there are many small cells. The main aim is to reduce the load on the macrocell base station. There arises a great value for authentication for users. It is assumed that in 5G, the users will be moving from one place to another with high speed. Also, it will enter the adjacent cell very easily due to area constraint. For a small cell or femtocell, the authentication of users would be of great importance because of high mobility. Such schemes should be present where fast authentication is done or one possible solution is the installation of identification or registration of users for a particular users. This concept of one identification proof is similar to CA (certification authority) but implemented on a large scale considering various factors while registering like MAC address, proof of identity, permanent address etc.

Chen et al. (2016) the User-Centric UDN concept also helps to reduce the burden of frequent authentication in microcell. A group of AP are created and assigned to a particular user. Whenever the mobile node moves to adjacent cell, he/she would not be requiring to prove his identity again. The UE proves his identity to only one AP which would be accepted by all the group.Only the group of AP are changed based on the location. It also benefits the passage of traffic without any
interruption and providing high data rate. For key management of UUDN, when the UE leaves or enters a particular APG. The new cipher and integrity keys will be provided or generated (Chen et al., 2016). Many light weight equipment will be covered in 5G for them light and integrated security technology is required (Chen et al., 2016) (Fig. 15).

3.4.4. Bandwidth spoofing

The bandwidth spoofing attack is more vulnerable as other types could be detected easily but in this the users do not have any idea, only the performance of the network degrades as shown in Fig. 16. It spoofs the bandwidth of the user and will transmit its own data. It is a type of passive attack in which no harm will be done to any device under a cell. The bandwidth spoofing attack will create more problem for D2D pairs. The famous gaming theory concept is used for its implementation and the success rate of attack depends on the number of times the disturbance is created to the target node.

3.4.5. Denial of service (DoS)

It is a type of attack in which users are denied from having access to the network. The attacker sends continuously the connection establishment request to the server and thus making it busy for the valid user. When the valid user arrives its request could not be served because the server is already preoccupied with the connection requests by the attacker.

This type of attack poses a serious threat to the network as it directly attacks the availability of the system or the device. By making the network unavailable, it aims at exhausting the resources at the victims side. In 5G, the mobile networks are extremely important as they have a limitation of power resources. For example, it is also carried out by mobile botnets. It could try to control the MME (mobile management entity) or HSS. Another scenario through which DoS attack could be mitigated in a wireless communication is radio interface jamming attack (Horn and Schneider, 2015). Major loss is done when attacker sends high transmitting power hence resulting in blocking of a particular frequency range. Due to the ultra-dense network property in 5G, the effect of jamming has a considerable impact on the users performance on large scale by the jammers where the resources of the attacker is not a major issue anymore.

3.4.6. Distributed Denial of service (DDoS)

It also aims at exhausting the resources of the network. But it is more complicated than DoS because the source of this attack cannot be detected very easily. It is distributed in nature. In this, the attacker captures a group of mobile devices and making them to do illegal activities placed at different locations.

The authors in Bilogrevic et al. (2015) discussed the issues with femtocells are considered and possible solutions are suggested where
<table>
<thead>
<tr>
<th>S. no.</th>
<th>Types of possible attacks</th>
<th>Objectives</th>
<th>Outcome</th>
<th>Possible solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Relay-based attack</td>
<td>To gain the control over the device. To exploit the integrity and confidentiality of users.</td>
<td>To control the flow of data through the relay. Resulting in eavesdropping. It can take the sensitive information. The MAC address is reconfigured.</td>
<td>Use WEP, WPA2 or WPA2 for encrypting the data. The information between the relay and base station should be encrypted.</td>
</tr>
<tr>
<td>2.</td>
<td>Rogue access point</td>
<td>To pretend as a legitimate AP. To access all the information and control over users (confidentiality). To transmit more power than the valid AP.</td>
<td>Results in transmission of data through false base station. Critical when hand over procedure is present.</td>
<td>The use of IDS is recommended if possible. To remove the default SSID of the access point.</td>
</tr>
<tr>
<td>3.</td>
<td>Authentication-based attack</td>
<td>The intruder will present itself as a valid client or try enter network. It can exploit authentication of users when mobility is high.</td>
<td>Shared key guessing Impersonation Attack MITM attack</td>
<td>Faster authentication scheme required than the rate at which adversary decodes the message. Use of pseudonym and signature based approach (Haus et al., 2017).</td>
</tr>
<tr>
<td>4.</td>
<td>Bandwidth spoofing</td>
<td>To get the knowledge about downlink/uplink mapping of SCA with Base station.</td>
<td>To make valid clients unavailable from the network. It is a type of DoS attack</td>
<td>Distributed IDS could be better alternative to detect anomalous behavior.</td>
</tr>
<tr>
<td>5.</td>
<td>DoS (Denial of service)</td>
<td>To make the network unavailable to users. To send huge amount of connection requests.</td>
<td>Identity attack Eavesdropping Packet injection and modification. Jamming attack for small cells by using SDR. Network unavailable IP spoofing</td>
<td>SAFH scheme for prevention of DoS (Li, 2011). Storing the personal data or highly confidential information in a very secure location such that each user has control over the data he/she has stored. By checking behavior of MAC layer by monitoring its parameters like PDR,carring sense time, etc (Kamel et al., 2016). Wireless Ad-hoc IDS formation for MANET or IDS present on the system of each user (Zhang and Lee; Sufatrio et al., 2015). IP spoofing</td>
</tr>
<tr>
<td>6.</td>
<td>Distributed DoS</td>
<td>To make the services of a device suspended temporarily. It floods the operating device with innumuous packet requests. Usually done by a group of compromised nodes.</td>
<td>Most common attack in mobile devices is the hotnets. Resource exhaustion. Bandwidth spoofing. Session Hijacking.</td>
<td>Same as required for Mobile Botnets and DoS.</td>
</tr>
<tr>
<td>7.</td>
<td>Location tracing</td>
<td>To know about the location of users and using their information to initiate another attack.</td>
<td>Inference attack by compromising privacy of users. Degradation in QoS by adversary to attacking node. Personal information leakage while using apps like We Chat, by visiting certain location, location of homes or office.</td>
<td>Before connection is established, a user needs to be properly authenticated by the apps manager. Proper encryption of Data or session establishment information exchanged between nodes and servers. Client side processing of critical data required. Random Routing Approach by phantom receivers (Koh et al., 2015). Faking of Source and destination location by randomly injecting dummy traffic (Mehta et al., 2012).</td>
</tr>
<tr>
<td>8.</td>
<td>Mobile botnet attack</td>
<td>Bot-Master sends spams or dodge users to install malicious software to their systems which further tries to compromise security of other nodes.</td>
<td>Launch of DDoS over air interface (Gerla et al., 2014).</td>
<td>Securing the information passed between source and server. Creating settings for security mechanism on a device (Hanna1 et al.). Analyzing untrusted Apps to prevent spreading of bots under a category of special systems as described in Hanna et al.. Detection of Similar functioning Apps by running particular code sequence (Hanna et al.).</td>
</tr>
</tbody>
</table>
the large scale deployment of less expensive nature of femtocells are prone to DoS and DDoS. It is known to occur in many companies having web-based services like yahoo, eBay or amazon. The effective suppression mechanism of these attacks is present when occur near to source of attack. We can say that adaptive scheme should be employed which would automatically/dynamically allot the temporary ID. With the help of Bluetooth, the behavior of nearby devices are analyzed like device speed, mobility, density etc and based on that the ID is changed (Bilogrevic et al., 2015).

3.4.7. Location tracing

Many mobile social networks applications demand the users location either in direct or indirect manner. They try to provide better services to users by exploring their nearby location and finding known contacts. A large number of society have a high level of involvement in these social networking sites and they tend to post the things occurring in their life. Nowadays, along with the information posted by the user, the location of the person is deliberate exposed to outside world. The most common application is the Facebook in which Geolocation Tags is present or the check-in services. It also reveals the mobility of users and try to guess the location of user. This attack not only exploits the location of user but also tries to get the sensitive information about the user like name, age interest, hometown. Li et al. (2016) in this paper, two data sets are collected from wifi of college campus and volunteers are picked which directly or indirectly shares there location. It is also mentioned in this paper that in Momo 80% of the tracking results can geolocate the victim in 40 m range.

The previous methods of location tracing of the users depend on phone call logs, GPS navigation system and application dependent on GPS tracking. The dense network in 5G aims to use devices that uses internet for data transfer. Using the MSN, the neighboring users also might get exposed to vulnerability. The adversary may use a novel approach to exploit the resources of the network. The mobility pattern and sensitive data (or demographic attributes) can be easily predicted. This could lead to phishing attack in which attacker can use the information like credit card number etc for his own benefit. Many solutions have been suggested to prevent users from sharing location intentionally or not. The users could restrict the applications from using his/her location. They could ask the user before sharing anything while running the application. It is also suggested that the most visited location by the user is closely related to the home or work area. Hence, it requires higher protection level. The regions where large users are present, they require lower protection level (Li et al., 2016). The attack could be generated in a manner in which firstly the densely populated area is selected like campus wifi. The attack on wifi could be easily made and hence all the information about the users are predicted by analyzing the traffic pattern.

3.4.8. Mobile botnet

A mobile botnet attack is defined as controlling the computers through remote access by instantly bot virus in then by either by transferring infected files through internet or any other physical means as shown in Fig. 17. It is the most common attack generated against the smart-phones. It is generally done to gain money by targeting the victim. It is mostly spread by maliciously sending unwanted software and users without having much knowledge run on the system. The threat is present in next generation mobile networks as most of the devices are connected through internet all the time and they act as a

![Fig. 14. Rogue access point.](image)

![Fig. 15. Typical attacks present in UDN.](image)

![Fig. 16. Bandwidth spoofing attack.](image)

![Fig. 17. Mobile Botnet attack in 5G.](image)
gateways to propagate easily through the network. One idea that could be used is by placing mobile devices behind the firewall. But for bothered, it proves as an easy task to cross this hurdle. Nowadays, only the web based botnet where they are connected to web servers are active and they play role as long as connection is maintained. The attack become widespread when the attacking node is one of the user from D2D pair. Hence, it infects or tries to control other users present in its pairs. The bots can also collect sensitive information about its neighboring pairs. In this way it can spread to a considerable range. The suggested solution is to use anti virus scanner which can scan incoming and outgoing messages. Another possible solution is turn off interfaces like Bluetooth, infrared or any wireless access point (Flo and Josang, 2009).

Gerla et al. (2014) have tested the vulnerability of air interface in 4G cellular network by launching the DDoS attack in order to check the number of devices effected by botnet attack. Such that denying services to the voice users and it effects around 3% of Quality of voice traffic which is a considering amount. This creates a major concern over the introduction of new mechanism to enable security for the critical information transfer over the wireless network.

3.4.9. Handover attack

For the security of users in ultra dense network where there is extremely high probability of handovers due to confinement of large number of small cells in a particular area could possibly be done by the approach of dynamic authentication schemes. One such scheme is the implementation of dynamic passwords having public key for light weight applications for this the requirement for certificate for authentication purpose would be less. There are handover procedures which require multihop and single hop transmissions. But we need to investigate on the security mechanisms of the multihop communication which includes the involvement of AP. In LTE-A, they have also assisted the use of relay in its architecture for frequent handovers for fast moving users. One such critical region for the attacker to increase the miss rate of handover. Or We can also say that the attacker can greatly affect the network by increasing the dropping rate of calls and hence decreasing its performance where relays security is compromised. So such novel scheme need to be designed for achieving effortless handover between the AP and Clients or among D2D pairs. However, some schemes have been proposed for LTE-A in both 3GPP and non-3GPP network but they have a major issues like incompatibility related to the use of public key cryptography as the main motive of the attacker is to exhaust the resources of the clients which are already limited in their power backups.

Khosroshahi et al. (2013) considering the already existing threats present in the LTE-A networks, we are assuming those things are still prevalent in the 5G architecture as well which includes the deficiency of backhaul security when keys are exchanged between the UE and eNB, desynchronization attacks i.e deployment of personal AP or eNB by the adversary and replay attack is introduced by the attacker by intercepting the encrypted handover request message between two communicating nodes.

3.4.10. Power saving attack

Most of the power consumed by the base station is mainly due to the control messages send to the users during sleep and idle mode. Only a little amount of power is consumed while transferring the data or voice messages to different users. During the power saving mode, the users tend to be most vulnerable to attack. The attacker tries to update the location and data arrival indication of control messages. After updating the location of device, the attacker will try to spoof the bandwidth or it could result in distributed DoS. Rengaraju et al. (2013) this type of attack exits in one hop transmission or we can say that users nearer to base station of microcell or access point can become victim to power saving attack. But for IEEE 802.16m it is possible to initiate this attack. In today world where everyone is doing work and focusing towards the methods of saving power. The distributed architecture of UDN in 5G and dense network where power constraints is a major issue, this attack could play a role in exhausting the resources.

3.5. Possible solutions of attacks in ultra-dense networks

The architecture of ultra-dense network incorporates various new technologies like IoTs and also various small cells having overlapping regions with the macrocell. The security architecture in 5G depends totally upon the applications which will be used in it. The increased dense network and indude of new applications also add to many vulnerability in 5G. This gives rise to many questions should new architecture of 5G be added in 4G having supported security. Another suggestion could be development of 5G and having backward compatibility with LTE. While designing of new security architecture few things should be kept in mind that it should not greatly affect performance of network and for limited power devices there should be only authentication required avoiding the encryption. The light weight authentication algorithms should be used while applying such that it will not exhaust its resources. Until now nothing much about the architecture of 5G have not been standardized by 3GPP. Researchers only have suggested the applications which are to be included in 5G based upon the requirements of users. The overall specifications of 5G by 3GPP are yet to be declared. All the issue discussed in Wang et al. (2014) need to analyzed but still there is much to do in the field of security as not much have been done. The deployment of ultra-dense network aims at increasing the quality of service which will increase the usability and security at a low cost of service. However, in this section we will be discussing the solution of expected attacks one by one. Among all the described attack above, denial of service is the most common and serious issue which needs to take care of and with the evolution of mobile generations the attacker will find somehow new method to implement it. These attacks are not much dominant up to 3G but with the advent of new technologies and involvement of IP address have exposed even the mobile communication with these vulnerabilities which are associated with computer networks. In Li (2011) the secret Adaptive frequency hopping (SAFH) technique is proposed for the prevention of DoS attack in which blacklisting of certain frequency components is done based on their behavior. In this method the BER of physical layer is calculated and its value is observed. Based upon the modulation techniques the frequencies of certain users are shut down and blacklisted. In this paper, the authors have compared the BER parameter of both the physical layer and application layer. It is observed that application layer tends to show deviation in behavior. Li (2011) the observed value of BER is 50 times more than the estimated value. The selection of modulation schemes is based on the techniques used in LTE Advanced. The level of precision of SAFH can be estimated by sending signals at different frequencies and the analyst can try to listen (or eavesdrop) for protection against denial of service.

The femtocells are prone to many new attacks in which new clients are added without any verification for them the clients should be registered first before entering in the network. Other attacks which could be possible like device impersonation, internet protocol attack, false location reporting. For a particular geographical area femtocells are deployed. So such scheme should be present in which physical tampering of device should not be there (Bilogrevic et al., 2010). In femtocells, for subscribers identity and location tracing prevention, there should be development of more dynamic and location aware protection. The protection of data of femtocells over the air interface can be done by encrypting the messages. But for small size, low power femtocells, this idea is not feasible as it could add an extra overhead on the performance.

The IP based threats can be resolved by implementing the IDS and
the best e
this there are various questions that need to be answered. In this paper, of either the house, o
mechanism as compared to RF based transfer for short range transfer
3.6. Visible light communication security challenges in 5G
in it (Mavoungou et al., 2016).

The most popular attacks against the physical layer are jamming and eavesdropping. Many schemes have been proposed by researchers in LTE-A for its prevention. We will be suggesting the schemes which could be helpful in ultra-dense in the coming section. For jamming, artificial noise security and security-oriented beamforming techniques could be possible solutions (Mavoungou et al., 2016). Also various types of jamming prevention techniques are present and each has its own level of feasibility and security levels. The main concern is that those schemes could be possible in our UDN or not. Does these schemes will remove the affect of intruder or the intruder itself? Like this there are various questions that need to be answered. In this paper, the best efforts have been given to resolve the issues and doubts up to a greater extend.

3.6. Visible light communication security challenges in 5G
For the 5G network, VLC serves as a better communication mechanism as compared to RF based transfer for short range transfer of files, data etc. The application of VLC is limited to only a small room of either the house, office or small academic region. Hence serving a small number of users. The special quality of VLC is that the communication can only be done if the receiver has a LOS path with the AP. The term used here is light which has the involvement of light i.e LED acting as a source. The transfer rate or the speed with which the transfer takes place depends on the alignment of the source. The main goal of communication system is to establish secure and high speed links without much delay in the connection. It uses the conventional OFDM multicarrier technology for achieving high data rates and to remove the effect of interference. There are considerable number of benefits VLC has as compared to RF based communication which are as follows:Operates in license free band with a range from 428 to 750 THz (Wu et al., 2014).

- Having less interference between the communication of indoor and outdoor interference.
- Transmission power required for the AP is less.
- High Spectral Efficiency

The requirement is to maintain LOS path between transmitter and receiver. Hence achieving large coverage area. Thus protecting the legitimate users from the eye of eavesdropper. Another issue of VLC is for mobile nodes. Due to extreme narrow Beamwidth and directional properties, the difficulty arises when the node is moving. Hence its properties is restricted to only stationary nodes. Another problem which could hinder the communication path between two nodes by the intruder is done either by blocking the communicating path or introducing some obstacle (Wu et al., 2014). The type of the antenna also plays a major role for achieving a better spectral utilization and energy efficiency. In this paper (Wu et al., 2014), they have also introduced the concept of Visual MIMO having camera receiver and an array of LED transmitter.

4. Proposed architecture
On the basis of the above study on security issues of the UDN in 5G networks. We are giving a proposal on the major security threats for UDN which would be affecting our network to a greater extent. There are 5 possible attacks that can be possible in UDN as per our proposed network model. In the Fig. 18, we are dividing our cell into different UDN regions each describing its own security flaws . As it is already understood by now that the major applications covered by 5G are: D2D pairs, small dense area, residential region, malls, cafeteria, buildings, IoT devices, medical applications and many more. However, the working of the conventional architecture of wireless communication is still the same despite the working frequency is changed with the increase in demand of high data rate through mm-wave and the introduction of massive MIMO. Keeping all these basic requirements in mind, we will be discussing each one of these security flaw one by one which are as follows:

**Case 1.** IP spoofing: the basic design of 5G architecture has used the IP based architecture approach where each and every device has its
own IP address. With such a great increase in the user density, it is a basic need for each and every person to get its own address. Such management of huge number of address is itself a very difficult task because it gives invitation to many attackers to hinder in the working of the network. One such major attack would be present is the IP spoofing which has its major impact on IoT devices. The increased number of small networks within a macrocell results in conflict with the IP addresses due to overlapping regions. Thus adversary tries to capture the packet from the source which contains the IP addresses of both sender and receiver by altering the source address. It is most frequent type of attack used in Denial of Service as the traffic volume to a particular network is such large that it does not care from where the response is coming. Hence compromising the privacy of the users.

**Case 2.** Interference management attack: UDN is equipped with an integration of large number of cells which are closely associated and many share a common region with one or more cells. Each cell has its own communication range like for a home network as depicted in Fig. 18 shares a common region with its neighboring cells. In this type of attack, the node which is present in the shared region is more suspected to attack by the attacker. It can easily propagate the damage of its attack to a wider range by any node present in the interference region. Here, we are assuming that the nodes which are present are having no movement.

**Case 3.** Handover Management attack: as presented in the proposed diagram that the user sharing the common region with two cells will be confused with whom he/she can establish connection as both the cell is sharing a major portion of their communication range. The user having a considerably optimum mobility from cell 1 to cell 2 will face session hijacking attack as during that short span time of key exchange, the attacker will try to steal the confidential information which would be forwarded to the further node receiving benefit from that information. During the movement from one area to another considerable drop in the value of SNR is expected as result of which valid user again tries to establish connection.

**Case 4.** Unauthorized cell identification: as it is already understood by now that increase in user density will increase in the number of SCA to cater with the increase in the capacity. The client who wants to connect to a SCA will remain in confusion with whom to connect. In other terms, particularly in UDN increase in SCA number gives an opportunity to the Adversary (or attacker) to create its own cell. When the valid client will enter the particular region, he/she will remain in confusion or unauthorized cell identification becomes a difficult task during the new connection establishment as shown in Fig. 18. This critical issue will provide an opportunity to the attacker to get the control over small cells. As these small cells are formed by users because they are unidentified by the AP.

**Case 5.** RFID Tag: this type of attack is most prevalent in IoT applications where the use of RFID tag has increased many times specially in surveillance application, shopping purposes or for vehicular communication. RFID tag contains all the basic information about a thing like taking a case of car trying to cross a toll booth. Firstly, it would be scanned RFID reader having all the information about a device which is then migrated to database center for cross-checking to check the authenticity. Here the confidentiality of the information needs to be maintained as the attacker can try to clone the tag or the information send from tag to reader could be overheard by the eavesdropper. If the efforts for encrypting the information is made, then this could provide chance to attacker to easily guess key as the RFID tags are having very less computational capability.

### 5. Conclusion

In this paper, a detailed survey has been done on the security issues of Ultra Dense Networks and the possible solutions to overcome such issues for 5th Generation wireless communication. With increase in demand by the users for high Quality of service with low latency has increased the need for such secure architecture with could meet the growth in rate by providing authentication, confidentiality, integrity and non-repudiation to the data. An emphasis on other security aspects have been done keeping in mind the impact of user and AP density and the amount of damage adversary can create in such a deployment scenario. We have tried to list out major possible attacking regions in UDN. However, the possibility is not limited to the names mentioned above. Before the testing of any solution for security, the knowledge for fundamental differences between the 4G and UDN based 5G are required in order to create a good level of results. Another aspects in UDN should be considered is the vertical densification which also increases. Secondly, the installation of many such new applications in the 5G architecture have open gates for security breaches for them also and the attacks attached with them. Numerous security challenges and open problems in UDN are presented in this survey in different subject.

### Appendix A

See Tables 9–11.

### Table 9

**On-going projects in 5G related security.**

<table>
<thead>
<tr>
<th>S. no.</th>
<th>Ref.</th>
<th>Work</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>(Shen et al., 2016)</td>
<td>Supported in part by NSF under Grants CNS-1117687 and CNS-1320736 and National Natural Science Foundation of China under Grants 61203036 and 61573103.</td>
</tr>
<tr>
<td>2.</td>
<td>(Wu et al., 2014)</td>
<td>Work supported by National Science Foundation for “The Cross-Ministry Ciga Korean Project” of Ministry of Science, ICT and Future planning.</td>
</tr>
<tr>
<td>3.</td>
<td>(Fan et al., 2015)</td>
<td>Supported financially by National Natural Science Foundation of China (Nos. 61303216 and 61373172), the china post doctoral Science Foundation funded project.</td>
</tr>
<tr>
<td>4.</td>
<td>(Zhang et al., 2016)</td>
<td>Work was supported by National Natural Science Foundation of China under grant 61571020, by National 973 project under Grant 2013CB836700; by National 863 project under Grant SS2015AA011306 and major project for Beijing Municipal Science &amp; Technology Commission.</td>
</tr>
<tr>
<td>5.</td>
<td>(Mingjun Wang and Yan, 2015)</td>
<td>Work was sponsored by Ph.D. Grant (JY0300130104) of Chinese Educational Ministry for Researchers from Abroad (JY0600132901), the grant of Shaanxi province for excellent researchers and Aalto University.</td>
</tr>
<tr>
<td>6.</td>
<td>(Mishra et al., 2004)</td>
<td>Received partial support from Australian Research Council Discovery Project ARC DP130101383 and further more.</td>
</tr>
</tbody>
</table>
Table 10
Standards on security.

<table>
<thead>
<tr>
<th>S. no.</th>
<th>Agency</th>
<th>Name of draft/white paper</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>NIST Special Publication</td>
<td>An Introduction to Computer Security: The NIST Handbook</td>
<td>Handbook designed by NIST provides a new insight by securing resources associated with computers. It provides the overview about security needs and approach for selection of certain security technique. It provides a baseline as it discusses various security benefits. The main motive of this documentation is to provide standardized approach to evaluate a system. It provides various security assessments for IT systems. They have also prepared questionnaires and simultaneous guidance on it. The effective risk management has been presented in IT systems from both theoretical as well as practical guidelines point of view. This document provides the information to various organizations about the capability of the LTE Technology. It does not take into non-3GPP networks, D2D, IoT etc. The detailed description about the security architecture of LTE Networks have been provided. The detailed description about security capabilities of Bluetooth have been done and methods to secure them. They have also highlighted security limitations in Bluetooth and security threats associated with them. Making deployment of small devices having low power resources easier, the need for light weight cryptographic technique is felt and questions have been developed in this draft before things are implemented. This draft outlines threats associated with mobile devices and security solutions attached with it especially beneficial to enterprise IT. This document is designed for efficient implementation, configuration, security etc of IDPS such that proper reports, events can be created. The general concepts related to security evaluation in IT and general model for evaluation of security properties for the products developed for IT sector.</td>
</tr>
<tr>
<td>2.</td>
<td>NIST Special Publication</td>
<td>Security Self-Assessment Guide for Information Technology System</td>
<td></td>
</tr>
<tr>
<td>3.</td>
<td>NIST Special Publication</td>
<td>Risk Management Guide for Information Technology Systems</td>
<td></td>
</tr>
<tr>
<td>4.</td>
<td>NIST Special Publication</td>
<td>Guide to LTE Security</td>
<td></td>
</tr>
<tr>
<td>5.</td>
<td>NIST Special Publication</td>
<td>Guide to Bluetooth Security</td>
<td></td>
</tr>
<tr>
<td>7.</td>
<td>NIST Interagency Report</td>
<td>Assessing Threats to Mobile Devices &amp; Infrastructure</td>
<td></td>
</tr>
<tr>
<td>8.</td>
<td>NIST Special Publication</td>
<td>Guide to Intrusion Detection and Prevention Systems (IDPS)</td>
<td></td>
</tr>
<tr>
<td>9.</td>
<td>ISO/IEC15408-1:2009</td>
<td>Information Technology security techniques evaluation criteria for IT security</td>
<td></td>
</tr>
</tbody>
</table>

Table 11
Standardization agencies.

<table>
<thead>
<tr>
<th>S. no.</th>
<th>Agency</th>
<th>Objective</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>5G ensure</td>
<td>Securing 5G networks</td>
</tr>
<tr>
<td>2.</td>
<td>NIST</td>
<td>Broader level of methodology for cybersecurity outcomes benefiting private organizations.</td>
</tr>
<tr>
<td>3.</td>
<td>ISO</td>
<td>Testing of different software applications in secure format</td>
</tr>
<tr>
<td>4.</td>
<td>IASME</td>
<td>Certification assurance for cybersecurity from small to medium enterprises.</td>
</tr>
<tr>
<td>5.</td>
<td>ISF</td>
<td>ISF published Standards of Good Practice containing list of best practices for Security.</td>
</tr>
</tbody>
</table>

References


Shen, W., Yin, B., et al., 2016. Secure Device-to-Device Communications Over WiFi Direct. IEEE.


---

Miss. Garima Chopra received the B.Tech degree in Electronics and communication from Shri Mata Vaishno Devi University, Jammu and Kashmir, India, in 2013 and M.Tech Degree Specialized in Communication and Information Technology (CIT) in Electronics and Communication Department from National Institute of Technology, Srinagar, Jammu and Kashmir, India, in 2016. She is currently pursuing the Ph.D. degree in Electronics and Communication Engineering at Shri Mata Vaishno Devi University, Jammu and Kashmir, India. Her research interest includes the security in emerging technologies of 5G wireless communication network. Currently she is doing her research work on Security issues of Ultra Dense Network in Fifth Generation wireless communication. She also worked on the security issues of Wireless Communication and their Security aspects. She has worked on Quality 5.0.2 simulation and Matlab Tool for Wireless Communication. Miss Chopra has received a Teaching Assistance from 2014 to 2016 through MIHRD and is currently a member of IEEE.

Dr. Rakesh J. Jha is currently an Assistant Professor in school of electronics and communication department, SMVD University Katra (J & K). He is carrying out his research in WIMAX and Security issues in the laboratory ECED Lab, SMVDU. Involved research topics include WIMAX performance analysis, LBRRA, power optimization and security analysis. He has done B.Tech in Electronics & Communication from Bhupal and M.Tech from NIT Jalandhar, INDIA. Received his Ph.D. degree from NIT Surat in 2013. Published more than 50 International Conference and Journal papers. His area of interest is Wireless communication, Communication System and computer network, and Security issues (Opti System). 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 award by ITU in Dec 2010, APAN fellowship in 2011 and student travel grant from COSMNET 2012. He is a member of IEEE, GSEFI and SIAM, International Association of Engineers (IAENG) and ACCS (Advance Computing and Communication Society).
Prof. Sanjeev Jain, born at Vidisha in Madhya Pradesh in 1967, obtained his Post Graduate Degree in Computer Science and Engineering from Indian Institute of Technology, Delhi, in 1992. He later received his Doctorate Degree in Computer Science & Engineering and has over 24 years’ experience in teaching and research. He has served as Director, Madhav Institute of Technology and Science (MITS), Gwalior. Presently, he is working as a vice chancellor at Shri Mata Vaishno Devi University, Katra. Besides teaching at Post Graduate level Professor Jain has the credit of making 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 major 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.