Asia Pacific Academy of Science Pte. Ltd.

Computer and Telecommunication Engineering 2024, 2(3), 2628
https://doi.org/10.54517/cte.v2i3.2628

Article

Adaptive beamforming approach for secure communication in 5G network

Arunima Sharma

Electronics and communication engineering, Shri Mata Vaishno Devi University, Katra 182320, India; arunimasharma7893@gmail.com

CITATION

Sharma A. Adaptive beamforming approach for secure communication in 5G network. Computer and Telecommunication Engineering. 2024; 2(3): 2628. https://doi.org/10.54517/cte.v2i3.2628

ARTICLE INFO

Received: 18 March 2024
Accepted: 16 July 2024
Available online: 29 July 2024

Abstract: The beamforming approach has been emerging as a very important concept for next generation networks. In addition to the improved channel capacity, spectral efficiency, energy efficiency, secrecy rate and secrecy outage probability, the upcoming fifth generation network mainly aims at enhancing the parameters of the channel for secure communication. In this paper, we have implied the allocation of resource blocks adaptively using HMM with a beamforming approach in an intruded network. A system model for secure communication in an intruded network has been discussed using a beamforming approach with the main motive being to provide a security scenario to the data which is transmitted over an unsecured channel in a network. In addition to this we have used the approach of HMM for allocating the resource blocks to the users which have been demanded and applied in order to avoid the intrusion and wastage of resource blocks.

Keywords: 5G; beamforming; HMM; resource blocks; spectral and energy efficiency; secrecy outage probability

1. Introduction

From the last few years, wireless communication technologies have surged at a very challenging rate, therefore crafting advanced and new services at a minimal cost. This forth hence resulted in an increment in demands of the subscribers like high data rates, improved spectral and energy efficiency, secure communication and secrecy outage probability. The most efficient way to tackle this problem is the usage of spatial processing [1]. Due to the increment in quality of subscribers and demands, there is a surge in the transmission quality and the coverage area, to fulfill these requirements smart antennas are used [2]. Adaptive Beamforming Approach is emerging as an optimal solution for fulfilling the surging demands of the subscribers. For various platforms of mobile technologies for example laptops, automobiles and cellular phones, smart antennas are being used [3]. Mostly the 3G systems operate in frequency bands of 3G Hz [2] and the 4G coins next stage of the cellular evaluation which do offer an efficient service of cellular technologies. This paper focuses on the algorithm which is required for Adaptive Beamforming in the radiation pattern of the antenna for secure communication.

It is an amalgamation of antenna arrays which do use the processors for digital signaling [4]. This paper also represents the improved channel capacity, spectral efficiency, energy efficiency, Secrecy rate and secrecy outage probability depicted via graphical analysis. There are different projects regarding the secure communication in 5G are mammoet [1], MCN [1], MOTO [1] which hence coined in different parts of the world. Work is being done on these projects in different parts of the world for the improved security scenario. The Adaptive Beamforming Approach that has been used in this paper for secure communication depicts two cases for the projection of the beam

that are; widening of beam and directivity. The results that have been depicted in this paper making a comparison study with and without using HMM which is used for adaptive allocation for resource blocks to the cellular users which have demanded the applications. A mathematical approach has been set up in this paper for coining different parameters of the network.

1.1. Background

The literature survey of more than hundred papers was conducted by me which motivated me to take a step further and do the work in this proposed scenario. This section essentially comprehends a survey of some of those papers which reflects the work that has already been done in the recent past in the field of security regarding wireless networks stating some of the recent technologies used. After the literature survey which has been done, it was very clear that security is the essential need of the hour. There is a growing need to adopt adaptive beamforming architectures in order to meet the increasing demands for improved capacity, higher data rates, higher quality of services and secured communication for the next-generation networks.

The emphasis on study of adaptive beamforming approaches started about two decades ago. Godara [5] suggested that there is a rapid growth in the communication technology which has led to increase in demands for higher data rate application with secured communication making adaptive beamforming approach all the more important. Different phenomena are included for securing the transmitting data. Han et al. [2] introduced the concept of cryptography into wireless systems for the transmission of data from base station to the users. Gandotra et al. [6] proposed an architecture for D2D WCN for a secured communication in which the users in the same proximity up to a certain distance will share the data hence reducing the probability of attacks. Ma and Tsudik [7] proposed the use of jamming technology in order to jam the signals from the attacker so that intrusion cannot take place and a secure communication of information can take place. From time to time the cell size, different techniques of cryptography, D2D WCN, resource block allocation, jamming techniques and beamforming techniques have been used for secure communication.

In the last decade, network deployment strategies have gained much attention including the focus on optimal cell size to improve the security scenario of a network. Claussen et al. [8] discussed the use of picocells and femtocells to decrease the path loss and improve the security aspect of the network and by improving the energy efficiency of the network. Derryberry et al. [9] proposed a new cellular architecture from optimal 3G network to adaptive beamforming network. Wang et al. [10] proposes separate architecture indoor and outdoor setups for 5G in order to facilitate the security aspects due to decreased path loss from the transmission by the indoor users.

Adaptive resource block allocation and beamforming has gained much attention in the past decade for securing the different scenarios of the different wireless communication networks. In the third-generation partnership project (3GPP) and long-term evolution-advanced (LTE-A) and IEEE 802.16j, beamforming standards have been detailed including the maximization of secrecy rate [11]. But many issues are still not discussed up to this point. Hence the allocation of resource blocks to the three demanded applications is explained in. Gupta and Jha [1] proposed a new architecture

regarding scaled beamforming Gupta and Jha [1] which hence is a modification to the zero-forcing beamforming. Nguyen et al. [12] explained the phenomena to maximize the secrecy rate by the joint information and jamming beamforming in cognitive radio networks. Chopra et al. [13] explained a new architecture for the security aspect in ultra-dense networks which hence was concentrated on the security issues of the physical layer [13]. Alotalbi and Hamdi [14] posited the concept of analyzing secrecy outage probability in a cooperative network for non-identically distributed Rayleigh fading channel but independent [14]. Zhang et al. [15] proposed a region-based beamforming for defining spatial secrecy outage probability.

1.2. Contribution

In this paper, our focus is on secure transmission of data in a Beamforming Approach for next generation networks. The system consists of a 5G network for D2D communication with Cellular users placed demanding for applications from Base Station. An Adaptive Beamforming Approach has been discussed in this paper for the security scenario in a network where applications are being demanded.

Secondly, in order to provide adaptive resource allocation of the subcarriers for the applications that have been demanded to all the nodes including the CUs, D2D pairs HMM has been used. The Hidden Markov model solves the allocation problem using a stochastic process and helps in training and maintaining of Base Station (BS), SCA and Relays based on various parameters and they in turn allocate power to their respective client nodes. The various parameters considered for power allocation are: node class, node distance, node SNR and application demanded by the client node.

Based on adaptive resource allocation and beamforming approaches we have proposed an algorithm for secure communication by decreasing the security issues. The second section contains a beamforming approach system model for secure communication for the next generation networks. It also provides a detailed mathematical analysis of the scheme adopted. Section 3 gives an account of the pseudo code of the algorithm used for secure communication with the flowchart used in the process. Section 4 embraces the imitation parameters cast-off and the exhaustive analysis of the results attained and the limitations related to the work. The supposition and the future research scope is debated in Section 5.

2. Secure communication scenario using beamforming approach

This section simply describes a system model and a mathematical analysis for secure communication of the next generation wireless network.

2.1. System model for secure communication

In a 5G Wireless Communication Network for a network of Device-to-Device communication where the applications are demanded by the cellular users from the base station. The three basic applications that can be demanded are data, voice and video from the base station. The resource blocks allocated to the respective user adaptively using HMM and adaptive Beamforming approach is implied further for secure communication after allocating the resource blocks to the users. Different parameters of a communication network like channel capacity, energy and spectral

efficiency, secrecy rate and secrecy outage probability are coined and a comparison has been made for the performance of the network between security scenarios with and without using HMM for allocating the resource blocks to the cellular users.

For the secure communication adaptive resource block allocation with adaptive beamforming approach is applied. In the adaptive beamforming there are generally two cases i.e.,

- Broadening of the beam where a larger area is secured in an intruded scenario, the distance of the intruded users is less from the base station.
- Directivity of the beam where a narrow area beam is used for the secure communication to the user which is a little away from the base station, the SNR in this case is greater as compared to the previous case.

Earlier the RBs allocated to the users demanding the applications equally which laid the probability of the intrusion in greater numbers. But in adaptive RB allocation using HMM, a probabilistic approach has been laid down for allocating the RBs according to the application which hence improves the security scenario and wastage of RBs. But the block size of the video application is still large in size which hence is laying the threat of intrusion. For removing the threat, adaptive beamforming approach has been implied for the secure communication of the data. The beam directivity is the phenomenon that has impinged in this case. After applying the adaptive beamforming approach different network parameters are coined for an optimal performance of the network. A comparison has also been made using and without HMM.

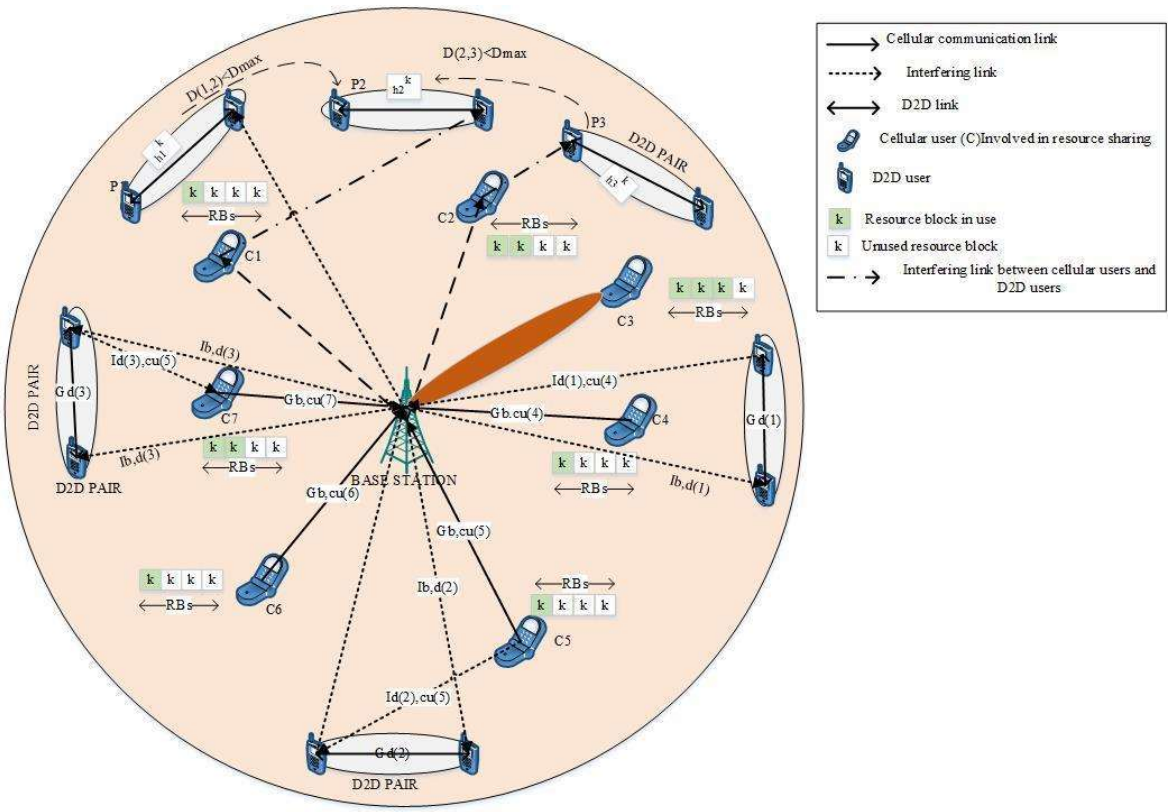

Figure 1. System model for secure communication.

2.2. Mathematical analysis for secure communication

A mathematical approach for adaptive beamforming has been proposed for coining the different parameters of the network to analyze the performance of the communication network under intrusion scenarios in **Figure 1**. In this scenario, a consideration has been made for a communication network of '*R*' radius where the BS is placed at the center allocating the RBs to the users which demanded the application by using HMM.

The channel gain taken between the cellular users as $G_{d,cu(b)}$ and at base station, the gain of interference link from BS to *a*-th D2D pair as $I_{b,d(a)}$, the interference link gain from *a*-th D2D pairs receiver to its CU be $I_{d(a),cu(b)}$. The transmitted power of the *a*-th D2D pair and *b*-th CU are depicted as $P_{d(a)}$ and $P_{cu(b)}$ respectively. The signal received at the BS of the CU and eavesdropper is represented by:

$$Y_R = \sqrt{P_{cu(b)}} H_{MN} S_{th} + \sigma_v \tag{1}$$

$$Y_{Re} = \sqrt{P_{txe}} H_{MNe} S_{the} + \sigma_v \tag{2}$$

where Y_R and Y_{Re} are the received signal strengths at BS of cellular user and eavesdropper, $P_{cu(b)}$ and P_{txe} are the transmission power from user and eves to BS, H_{MN} and H_{MNe} are the impulse responses of the channel for user and eves, S_{th} and S_{the} are the signal strength transmitted by user and eves.

The SNR of the *b*-th users is:

$$SnR = \frac{P_{r,cu(b)}}{\sigma_v} \tag{3}$$

where $P_{r,cu(b)} = P_{cu(b)} - P_l$.

Hence the channel capacity according to the Shannon's capacity will be:

$$C_{Hm}{}' = BW log_2(1 + SnR) \tag{4}$$

The SINRs of *b*-th cellular user and are stated as:

$$cu(b) = \frac{P_{cu(b)} X\ G_{d,cu(b)}}{\sigma_v + P_{d(a)} X\ Rs'\ X\ I_{d(a),cu(b)}} \tag{5}$$

σ_v is the noise variance and Rs' being the reuse component of RBs of the CUs.

Directivity phenomena

A directive antenna is used with varying beam-width for adaptive beamforming approach. For the mathematical proposal the gain of the directive antenna is considered as:

$$gn(\theta) = 1 + d^* \, cos\, cos(m\theta) 0 \le d^* \le 1, m \in N^+ \tag{6}$$

gn is the gain function and d^* is the beam-width

The D2D pair set is $d = \{1, 2, \ldots, D\}$. The Cellular user set is Cu = $\{1, 2, \ldots, c\}$. The allocation of RBs to the CUs is done periodically as Rbs = $\{1, 2, 3, \ldots, r\}$. The transmission power is P_B^*. The set of applications demanded App = $\{ap_1, ap2, ap3\}$.

The iterations are considered as set $q = \{1, 2, \ldots, Q\}$. At the receiver the SINR of the *a*-th D2D pair which is sharing *k*-th RB of *b*-th user, $j \in$ d, $k \in$ Rbs, $i \in$ Cu, given for every iteration as:

$$sinr_a^{k,b} = \frac{P_a^{k(b)} \times h_a^{k(b)}}{\sigma_v + \alpha_t} \tag{7}$$

α_t depicts the total interference that is encountered by the *a*-th D2D pair.

Hence the SNR received by the eavesdropper will be:

$$SnR' = \frac{P_{r,E}}{\sigma_v} \tag{8}$$

where $P_{r,E} = P_{txe} - P_l$.

Hence the channel capacity according to the Shannon's capacity will be:

$$C_{HmE}'=BWlog_2(1 + SnR') \tag{9}$$

The spectral efficiency of normal channel expressed in bps/Hz and is calculated as:

$$S.En = \frac{C_{Hm}'}{BW} \tag{10}$$

The spectral efficiency of intruded channel expressed in bps/Hz and is calculated as:

$$S.Ee = \frac{C_{HmE}'}{BW} \tag{11}$$

The energy efficiency of normal channel expressed in Mbps/J and is calculated as:

$$E.En = \frac{C_{Hm}'}{P_{cu(b)}} \tag{12}$$

The energy efficiency of intruded channel expressed in Mbps/J and is calculated as:

$$E.Ee = \frac{C_{HmE\prime}}{P_{txe}} \tag{13}$$

So hence the secrecy rate is stated as:

$$SRt = C_{Hm}' - C_{HmE}' \tag{14}$$

In order to achieve a high desirable level of secrecy rate, physical layer security serves as the optimum solution. Hence secrecy outage probability is given by:

$$P_{sC} = P_r\{C_{HmE}' < R_{RTn}' - R_c'\} \tag{15}$$

$$P_o = 1 - P_{sC} = 1 - P_r\{C_{HmE1}' < R_{RT1}' - R_c'\}P_r\{C_{HmE2}' < R_{RT2}' - R_c'\}P_r\{C_{HmE3}' < R_{RT3}' - R_c'\} \tag{16}$$

where R_{RT}', R_{RT2}' and R_{RT3}' are the code transmissions of data rates of U(1), U(2) and U(3).

So hence the secrecy is maintained after adaptive resource allocation but due large size of the RB of the video application, so to protect the channel from being intrude the phenomena of beamforming will be applied. The signal received at the base station is represented by:

$$Y_{rb*} = \sqrt{P_{cu(b)b*}}H_{Mb*}S_{tb*} + \sigma_v \tag{17}$$

$$Y_{rb*e} = \sqrt{P_{txb*e}}H_{Mb*e}S_{tb*e} + \sigma_v \tag{18}$$

The SNR will be:

$$SnR'' = \frac{P_{r,cu(b)b*}|h_0|^2}{\sigma_0} + gn(\theta) \tag{19}$$

where $P_{r,cu(b)b*} = P_{cu(b)b*} - P_l$, h_0 is the channel coefficient.

Hence the channel capacity according to the Shannon's capacity will be:

$$C_{HBm} = BWlog_2(1 + SnR'') \tag{20}$$

The SINR of the b-th cellular users is:

$$cu(b)b* = \frac{P_{cu(b)b} * W_b^H g^s_{bcu(b)w(b)}}{\sum_{b*} \quad P_{cu(b)b*}W^H_{b*}g^I_{abwb*} + \sigma_v} \tag{21}$$

$P_{cu(b)b} * W_i^H g^s_{b\prime cu(b)w(b)}$ is the desired power at the CU.

$\sum_{b*} \quad P_{cu(b)b*}W^H_{b*}g^I_{abwb*} + \sigma_v$ is the interference power from the BS to cu.

The SNR for the eve is:

$$SnR''' = \frac{P_{r,E(b)}|h_0|^2}{\sigma_v} + gn(\theta) \tag{22}$$

where $P_{r,E(b)} = P_{txb*e} - P_l$, h_0 is the channel coefficient.

Hence the channel capacity according to the Shannon's capacity will be:

$$C_{HBmE} = BW log_2(1 + SnR''') \tag{23}$$

The spectral efficiency of beamforming channel expressed in bps/Hz and is calculated as:

$$S.Eb = \frac{C_{HBm}{}'}{BW} \tag{24}$$

The Energy efficiency of beamforming channel expressed in Mbps/J and is calculated as:

$$E.Eb = \frac{C_{HBm}{}'}{P_{cu(b)b*}} \tag{25}$$

So hence the secrecy rate so obtained in this case is:

$$SRt = C_{HBm} - C_{HBmE} \tag{26}$$

Considering a network (AWGN) the eavesdroppers which are the adjoining will experience nominal path loss among the other eavesdroppers. Hence, the secrecy capacity will be determined with respect to the nearest eavesdroppers, such in that case the channel is greater than the given threshold $R_c \geq 0$ which is hence referred as Secrecy Non-Outage Probability and given as:

$$P(R_c{}') \triangleq P_r\{SRt > R_C{}'\} \tag{27}$$

$$\triangleq \left\{ log_2 \left(\frac{\delta^{-1} + r_{BS}^{-\alpha}}{\delta^{-1} + r_E^{-\alpha}} \right) > R_c{}' \right\} \tag{28}$$

$\delta = \frac{P_T}{\sigma}$, α is the path loss exponent, $r_{BS}^{-\alpha}$ is the distance between base station and cellular user, $r_E^{-\alpha}$ distance between base station and eves but there are many external factors with the intrusion attacks which does not support the SR and hence there is a decrease in the secrecy rate and hence that phenomena are called as Secrecy Outage Probability.

$$P_{outage} = P_r(SR < R_c) \tag{29}$$

$$P_{outage} = 1 - P(R_c) \tag{30}$$

As to study the probabilistic approach for allocating the RBs to the different cellular users demanding the different applications for secure communication, Hidden Markov Model in this paper has been discussed. BS controls the scheduling of the CUs. The representation of the HMM is done by the set of parameters P_R; set of states S_T [16]. The representation of the state diagram as: The base station (BS) and cellular users (CUs).

The representation of parameters by the matrices of probability as π, TP, EP.

$$P_R = \{\pi, TP, EP\} \tag{31}$$

Probabilities that are prior π hence giving the first state. Likelihood of the observation is represented by probabilities of emission [EP] and transition of one to another state is represented by the probabilities of transmission as [TP]. The process of HMM is usually characterized by sequence of observation $S_B = \{S_{B1}, S_{B2}, \ldots S_{Bn}\}$ and sequence of hidden state, $H_S = \{H_{S1}, H_{S2}, \ldots, H_{Sn}\}$. The probability sequence of hidden states is a product of probabilities of transition.

$$P(P_R) = \pi_{1H_S} \Pi_{N=1}^{n-1} \alpha_{H_{Sn}}, \alpha_{H_{Sn+1}} \tag{32}$$

Likelihood the observation sequence will be:

$$P(H_S, P_R) = \prod_{N=1}^{n} \quad P(S_{B\,n} | H_{S_n}, P_R) \tag{33}$$

Known prior to the RB allocation process is their observations. The set of applications demanded by App and their priorities are already known. Now by applying this phenomenon there is less chance of the spoofing of the data and voice RBs as due to small size resulting from adaptive resource block allocation. But still the RBs of video application is still under threat due to its large size. Hence here we can impinge the phenomena of beamforming.

As beamforming phenomena dedicate the beam of information from the base station to the user which demanded the application respectively. As there is deployment of multiple antennas at the base station and the application is demanded (video) via U(3) so hence there will be a dedicated beam projected. Earlier at the BS an omni-directional antenna was present for the allocation of the RBs but in this case, directive antenna is used at the BS for the RBs allocation and hence it results in difficulty for the intruder to eavesdrop the information.

The various parameters that are to be included via using the approach of HMM. The different parameters are as follows:

- The number of nodes.
- The types of nodes.
- The type of applications demanded by the client nodes.
- Resources blocks allocated to the client nodes.

Here in this scenario the resource blocks allocated to the respective user demanded the applications amongst video, voice and data adaptively.

2.3. Transition probability matrix for secure transmission of data

The HMM model used in this paper to depict the transition probabilities that the information is transferred from one CU to another according to the applications demanded by them. The subcarriers used for text and call are less as compared to video's subcarriers.

In the scenario for this paper, an adaptive resource allocation approach has impinged for the process of allocating the RBs to the CUs which demanded the application accordingly. The three users which are depicted as User 1, User 2 and User 3 demand data, voice and video applications as shown in **Figure 2**.

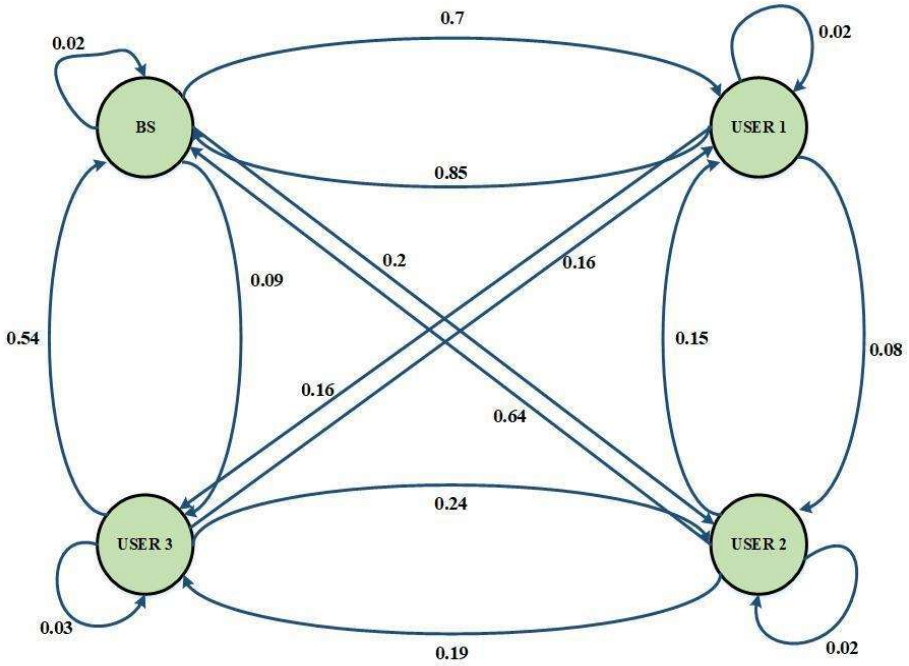

Figure 2. State diagram for secure transmission of data using HMM.

The transition from one to another state is depicted in **Table 1**.

Table 1. Transition probabilities.

Demand	**Response**			
	Base station	**Video client, User 1**	**Voice client, User 2**	**Data client, User 3**
Base station	0.02	0.7	0.2	0.09
Video client	0.85	0.02	0.08	0.16
Voice client	0.64	0.15	0.02	0.19
Data client	0.54	0.16	0.24	0.03

The Adaptive RB allocation is useful for the secure communication and to avoid the wastage of the RBs.

3. Realization and representation of objective

In this section, the pseudocode of the presented scenario for secure communication in this paper has been mentioned as for the optimized performance of the network.

Pseudo code 1: for realizing the scenario for D2D communication and cellular networks (depicted in **Figures 3** and **4**).

- Step 1: Input the parameters.
  Base Station: P_B, P_T, P_r, P_l
  Cellular user: P_a, r
  D2D users: P_B^{max}
  Channel: n, σ_0, R, q, A_p, B
- Step 2: Initialization.
  Generate the random user locations within a radius R for m iterations

Initializing the number of cellular users, hence c = 0/* All the cellular users indices are in set c*/

Initializing the number of D2D pairs, hence D2D pair = 0/*All D2D pairs indices are in set d*/

- Step 3: Check the users forming D2D pairs and deployment of the cellular users.

  for a = 1:n

  for b = 1:n

  Compute the distance with following equation:

$$\text{d (a,b)}=\sqrt[2]{(X\_loc_{(a)} - X\_loc_{(b)})^2 + \left(Y\_loc_{(a)} - Y\_loc_{(b)}\right)^2}$$

  check for D2D pair formation:

  if d (a,b) ≤ d_0

  Pair = pair + 1/*formation of a pair; hence update the pair in set d*/

  else

  $c = c$ + 1/* formation of a cellular user; hence update the user in c*/

  end

- Step 4: Computation of different channel parameters.

Different channel parameters like path loss, SNR, channel capacity, secrecy rate, spectral efficiency, secrecy outage probability and energy efficiency are computed and their respective values are plotted.

Pseudocode 2: for resource allocation by using hmm (in **Figure 5**)

- Step 1: Training of the data and calculation of prior probabilities.

  Computation of the set of probabilities and training of the data.

- Step 2: Specifying the Applications.

  Applications should be specified in the descending order of priority.

$$A_{\text{video}} > A_{\text{voice}} > A_{\text{data}}$$

- Step 3: Decide the number of RBs that should be allocated.

Allocation of the RBs is preferred adaptively within concern to the applications that are demanded and their priority. The value of 'k' depends on the application that has been demanded.

- Step 4: SNR and throughput computation which is based on the adaptive RB allocation.

Obtain the values of SNR and throughput from the trained data and distributed probability.

Pseudocode 3: for beamforming approach (in **Figure 6**)

- Step 1: Specifying the applications.

  Applications are specified in the descending order of the priority.

$$\text{A}_{\text{video}} > \text{A}_{\text{voice}} > \text{A}_{\text{data}}$$

- Step 2: Beamforming Approach is applied for RB allocation.

In the approach of adaptive beamforming, a directive and dedicated beam of RBs is allocated to the cellular users demanding video application.

- Step 3: SNR computation based on beamforming approach with respect to directivity.

Obtain the values of SNR from the trained data and plot the values by comparing them with earlier values.

- Step 4: Channel Capacity and secrecy rate computation.

Compute both the parameters and compare with previous values. Plot the resultant values.

- Step 5: Compute the secrecy outage probability.

Obtain the values of SOP and compare it with earlier values. Plot the resultant values.

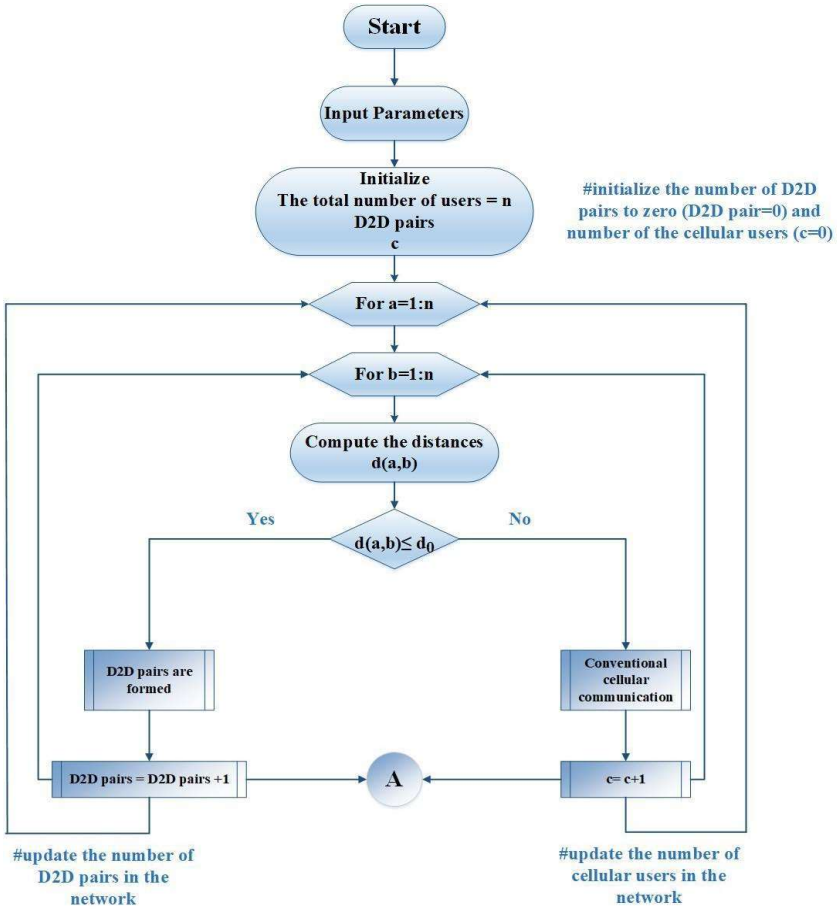

Figure 3. Flowchart for deployment of D2D pairs and cellular users.

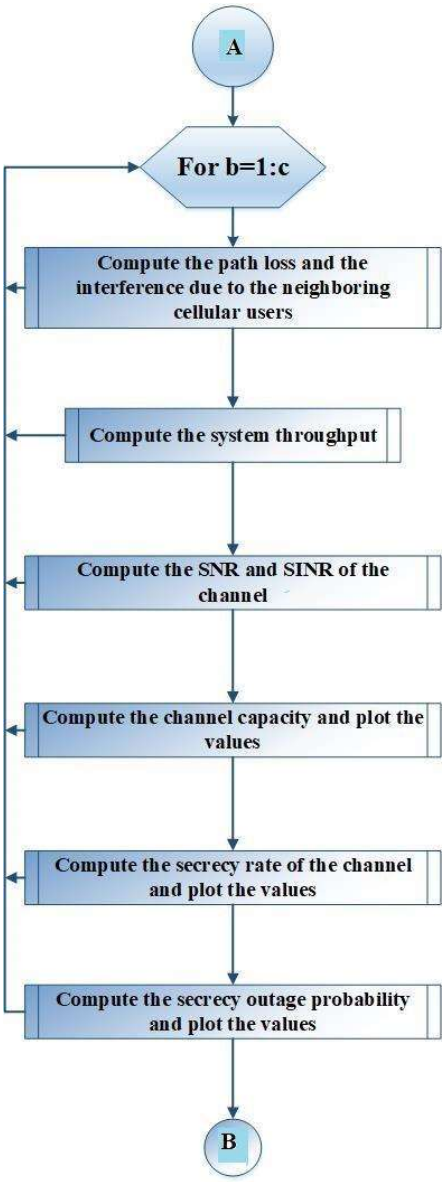

Figure 4. Flowchart of computing different parameters of the channel.

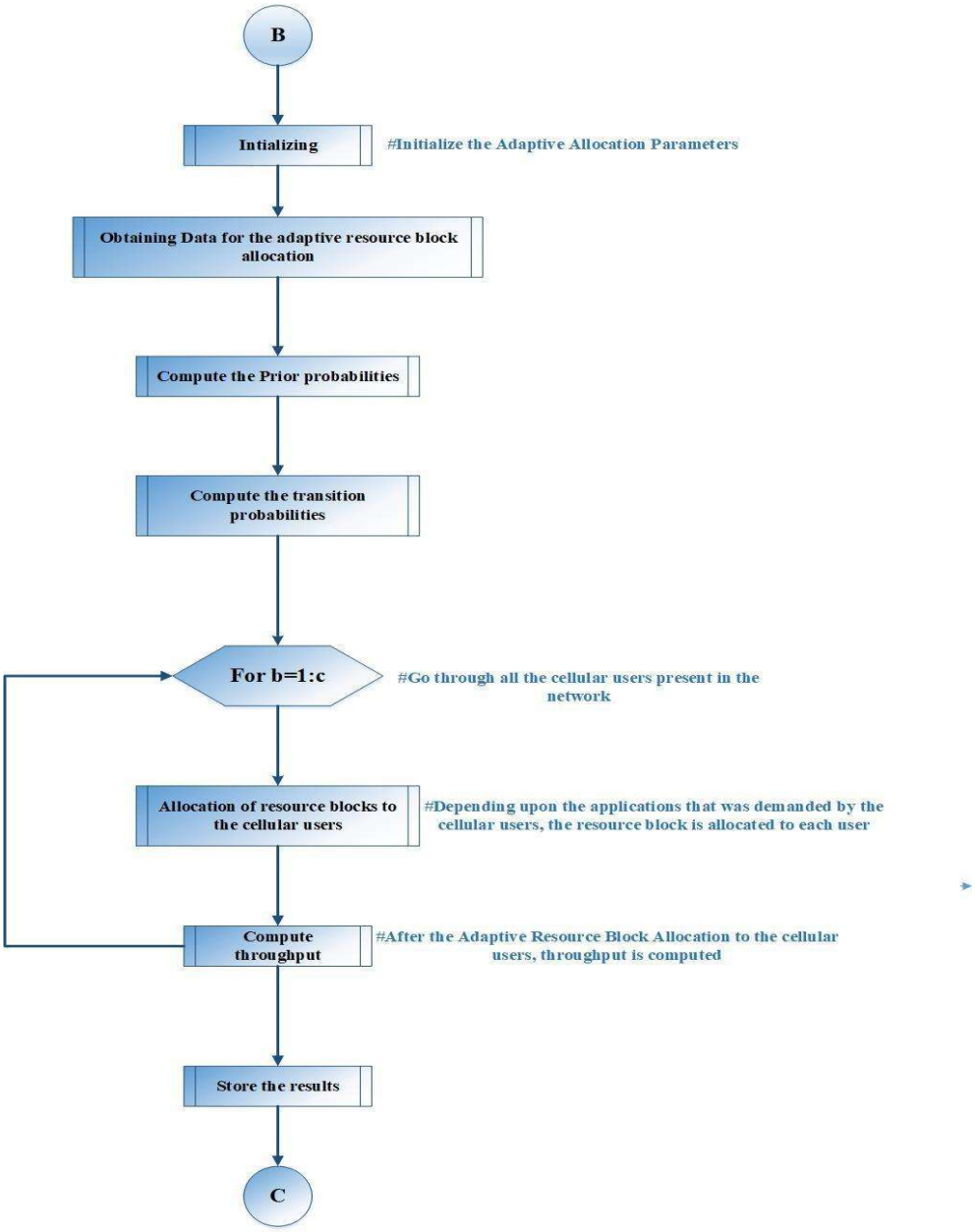

Figure 5. Flowchart for adaptive resource allocation.

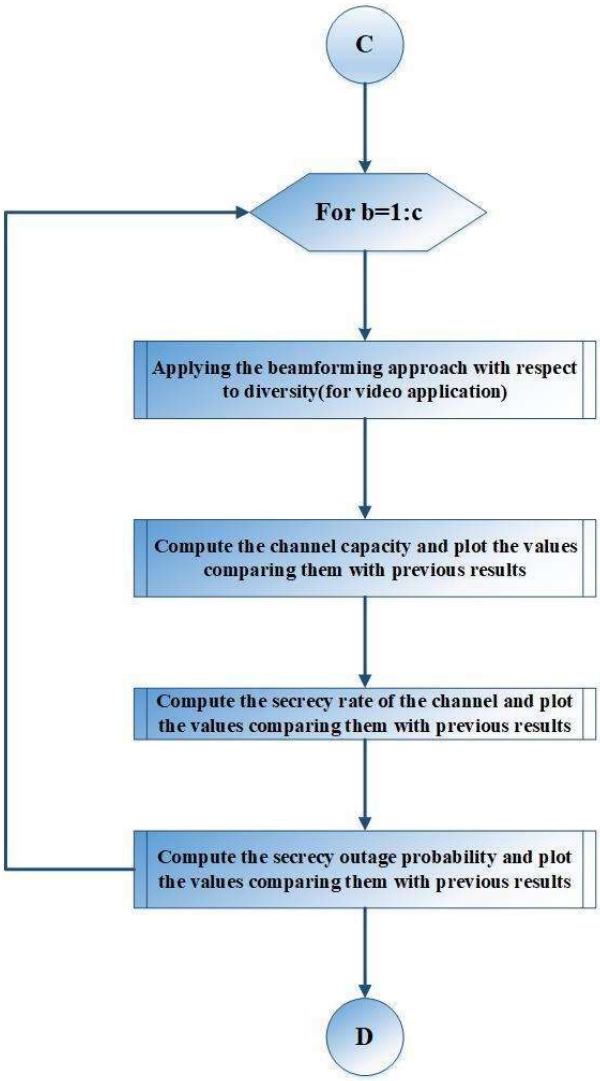

Figure 6. Flowchart for beamforming approach.

4. Simulation parameters and results

This section of the paper contains the different simulation parameters to evaluate the performance of the different parameters of the network. After the RB allocation by using HMM, beamforming approach has been introduced with respect to adaptive approach which hence is used to enhance the performance of the network. The parameters used in our simulation are listed in **Table 2**.

Table 2. Simulation parameters.

S.no.	Simulation parameters	Value
1	Carrier frequency (GHz)	2.5
2	Total bandwidth (MHz)	10
3	Transmit power from base station (dBm)	43
4	Path loss exponent	2
5	Noise figure dB	5

Table 2. (*Continued*).

S.no.	Simulation parameters	Value
6	Number of users	50
7	Number of Eavesdroppers	5
8	Number of subcarriers in the LTE-like system	600
9	Subcarrier bandwidth (KHz)	300
10	Radius (m)	300
11	Antenna gain (dBi)	20
12	Resource block bandwidth (KHz)	185
13	Path and penetration loss at distance *d* (km)	$148.1 + 37.6log_{10}(d)$ dB
14	Noise floor (dBm)	$-174 + 10log_{10}(subcarrier\ bandwidth) + noise\ figure$
15	Location of base station	(0,0)
16	QoS constraint	2 bits/s/Hz per user
17	Channel Capacity	$Blog_2(1 + snr)$
18	SINR constraints	$(2^{QoS\ constraint-1}) \times ones(number\ of\ users, 1)$
19	Noise Spectral density, σ_0	−174 dBm/Hz
20	Threshold Distance, d_0 (m)	20

The results that are so obtained by obtaining and implying these values are with the help of MATLAB. Different parameters that have been checked in this paper are given as:

4.1. Channel capacity

The effect of use of a directive antenna and HMM at the Base Station is examined by analyzing the channel capacity, spectral and energy efficiency, secrecy rate and secrecy outage probability. As already stated, there is a random deployment of nodes in the wireless network which results in the formation of cellular users and D2D pairs at every instant. The users which do meet the proximity criteria are successful to form D2D pairs, while the rest of the users that remain unpaired, and hence do operate as the cellular users working in the cellular mode. A comparative study has been made for with and without using HMM. The number of cellular users deployed in the network is 50.

Figure 7 clearly describes the deployment of the cellular users and Eavesdroppers in a wireless communication network depicting that the network scenario proposed in this thesis around 300 m radius with the BS placed at the center (0,0) is under threat. The transmission of the data from the Base Station to the cellular users is intruded by different attacks prevailing in the wireless communication network.

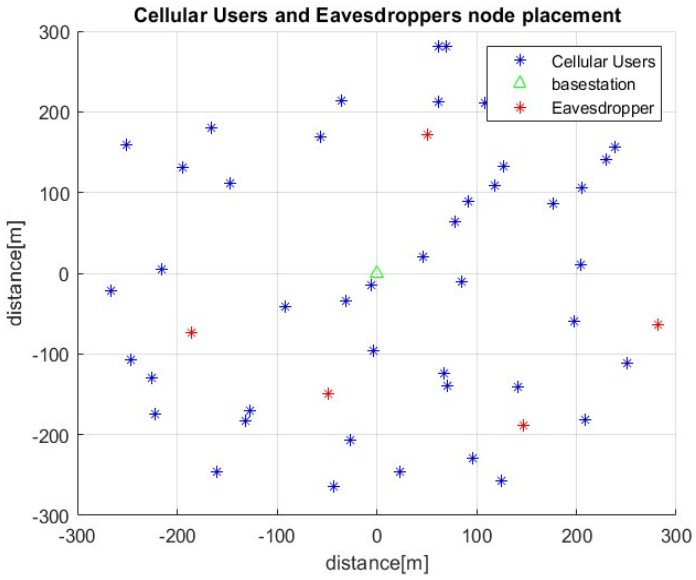

Figure 7. Deployment of nodes.

Figure 8 clearly depicts the channel capacity analysis with the respective SNR. The comparison is made with the normal channel capacity, channel capacity when the eavesdropper attacks or intrudes the transmission of data from the Base Station to the cellular users that demanded the application and the channel capacity by using the beamforming approach with respect to the diversity with the maximum rate of 85 Mbps. By adapting the beamforming approach, we had an increased channel capacity as compared to the channel capacity of the normal channel and the values are depicted in **Table 3**.

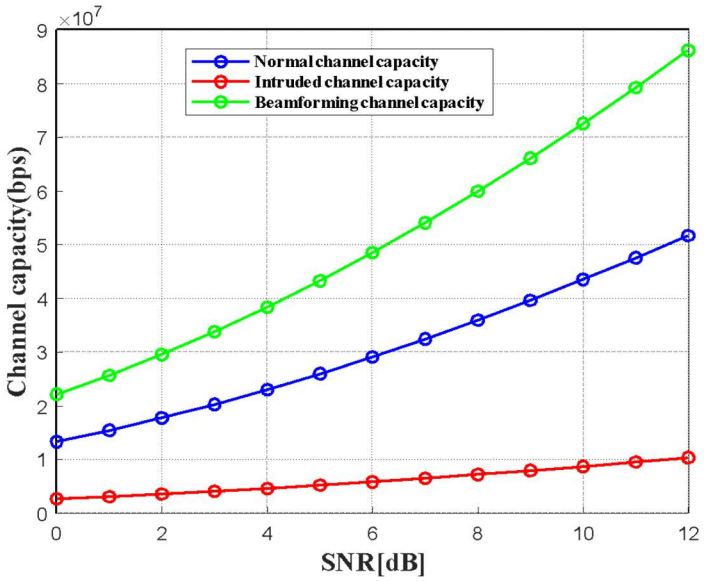

Figure 8. Comparison of channel capacity and SNR.

Table 3. Values of channel capacity.

S.no.	Number of iterations	Different channels	Maximum channel capacity
1	100	Normal channel	50.97 Mbps
2	100	Intruded channel	11 Mbps
3	100	Beamformed channel	85.2 Mbps

Figure 9 clearly depicts the channel capacity analysis with the respective SNR using HMM. The comparison is made with the normal channel capacity, channel capacity when the eavesdropper attacks or intrudes the transmission of data from the Base Station to the cellular users that demanded the application and the channel capacity by using the beamforming approach with respect to the diversity with the maximum rate of 102 Mbps. By adapting the beamforming approach, we had an increased channel capacity as compared to the channel capacity of the normal channel and the values are depicted in **Table 4**.

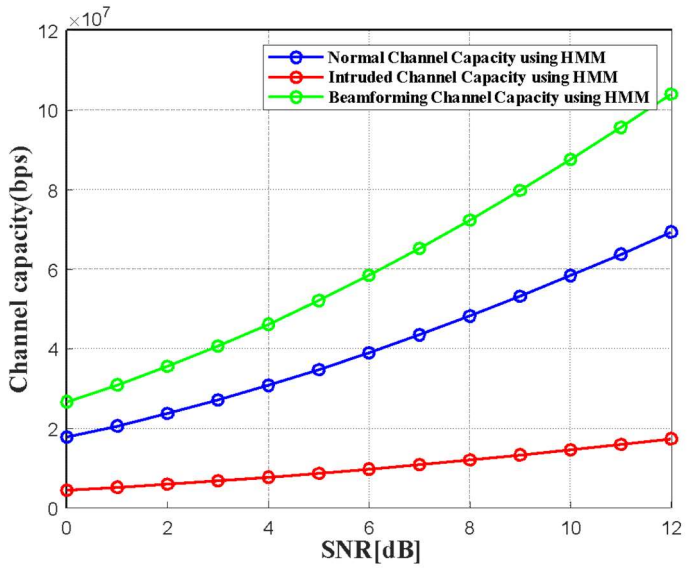

Figure 9. Comparison of channel capacity and SNR using HMM.

Table 4. Values of channel capacity using HMM.

S.no.	Number of iterations	Different channels	Maximum channel capacity
1	100	Normal channel	64.3 Mbps
2	100	Intruded channel	18.2 Mbps
3	100	Beamformed channel	102.1 Mbps

4.2. Spectral efficiency

Figure 10 clearly depicts the spectral efficiency of the channel with respect to SNR. As we know that spectral efficiency is defined as the information rate that is to be transmitted over a specified given bandwidth for a specific scenario of wireless communication network. The main objective of this phenomena is to measure how efficiently a frequency spectrum that is limited, be utilized by physical layer protocol and somehow by media access control. In order to reach up to the desired requirements of high spectral efficiency, low latency, high reliability, high throughput; a

combination of NOMA scheme and many other technologies. The figure describes the spectral efficiency analysis with SNR. The comparison has been made with the normal channel spectral efficiency, spectral efficiency of the channel after the attack or intrusion and the spectral efficiency of the channel applied with the beamforming approach. The values in this process are measured in bps/Hz. By adapting the beamforming approach, we had an increased spectral efficiency as compared to the spectral efficiency of the normal channel and the values are depicted in **Table 5**.

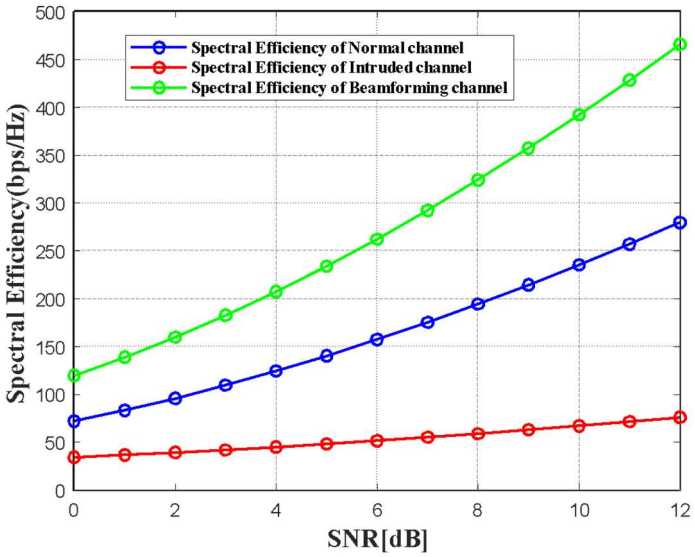

Figure 10. Comparison of spectral efficiency and SNR.

Table 5. Values of spectral efficiency

S.no.	Number of iterations	Different channels	Maximum spectral efficiency
1	100	Normal channel	256 bps/Hz
2	100	Intruded channel	50.2 bps/Hz
3	100	Beamformed channel	452 bps/Hz

Figure 11 clearly depicts the spectral efficiency of the channel with respect to SNR using HMM. As we know that spectral efficiency is defined as the information rate that is to be transmitted over a specified given bandwidth for a specific scenario of wireless communication network. The main objective of this phenomena is to measure how efficiently a frequency spectrum that is limited, be utilized by physical layer protocol and somehow by media access control. The figure describes the spectral efficiency analysis with SNR. The comparison has been made with the normal channel spectral efficiency, spectral efficiency of the channel after the attack or intrusion and the spectral efficiency of the channel applied with the beamforming approach. The values in this process are measured in bps/Hz. By adapting the beamforming approach, we had an increased spectral efficiency as compared to the spectral efficiency of the normal channel and values are depicted in **Table 6**.

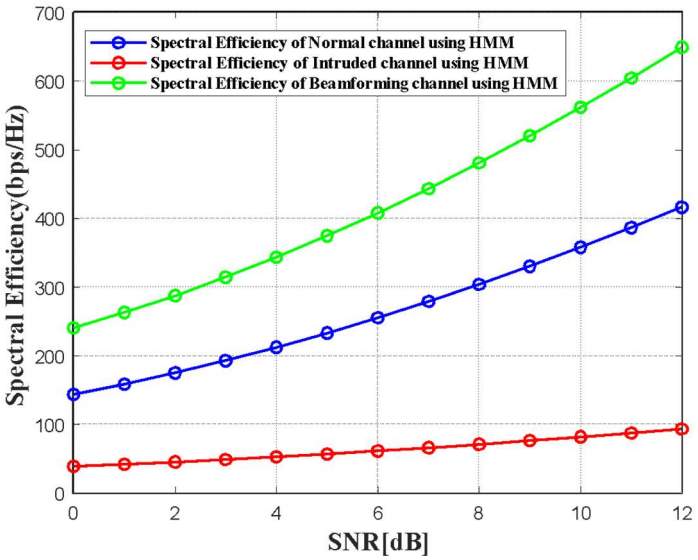

Figure 11. Comparison of spectral efficiency and SNR using HMM.

Table 6. Values of spectral efficiency using HMM.

S.no.	Number of iterations	Different channels	Maximum spectral efficiency
1	100	Normal channel	432.1 bps/Hz
2	100	Intruded channel	99.7 bps/Hz
3	100	Beamformed channel	666 bps/Hz

4.3. Energy efficiency

Figure 12 clearly depicts the energy efficiency of the channel with respect to SNR. As we know that energy efficiency is defined as a simple approach which describes how efficiently the energy can be utilized in order to preserve the energy in a network. The main objective of this phenomena is to measure how efficiently the energy in the network can be preserved for increasing the life of hand-held technologies.

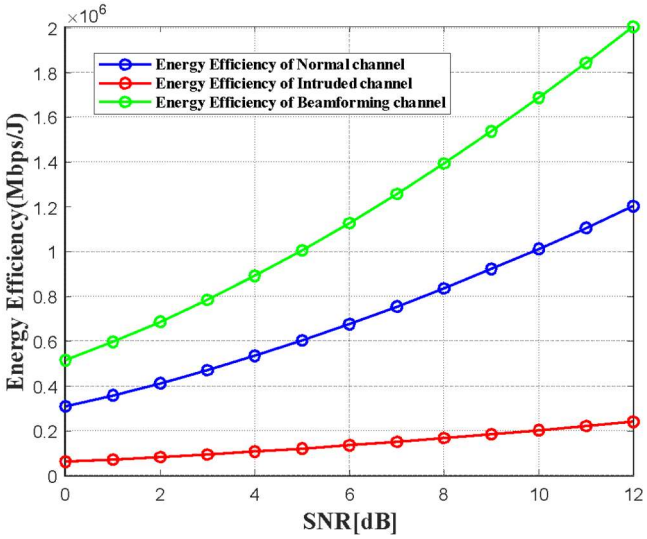

Figure 12. Comparison of energy efficiency and SNR.

The figure describes the energy efficiency analysis with SNR. The comparison has been made with the normal channel energy efficiency, energy efficiency of the channel after the attack or intrusion and the energy efficiency of the channel applied with the beamforming approach. The values in this process are measured in bps/J. By adapting the beamforming approach, we had an increased energy efficiency as compared to the energy efficiency of the normal channel and the values are depicted in **Table 7**.

Table 7. Values of energy efficiency.

S.no.	Number of iterations	Different channels	Maximum energy efficiency
1	100	Normal channel	1.18 Mbps/J
2	100	Intruded channel	0.22 Mbps/J
3	100	Beamformed channel	1.97 Mbps/J

Figure 13 clearly depicts the energy efficiency of the channel with respect to SNR using HMM. As we know that energy efficiency is defined as a simple approach which describes how efficiently the energy can be utilized in order to preserve the energy in a network. The main objective of this phenomena is to measure how efficiently the energy in the network can be preserved for increasing the life of hand-held technologies.

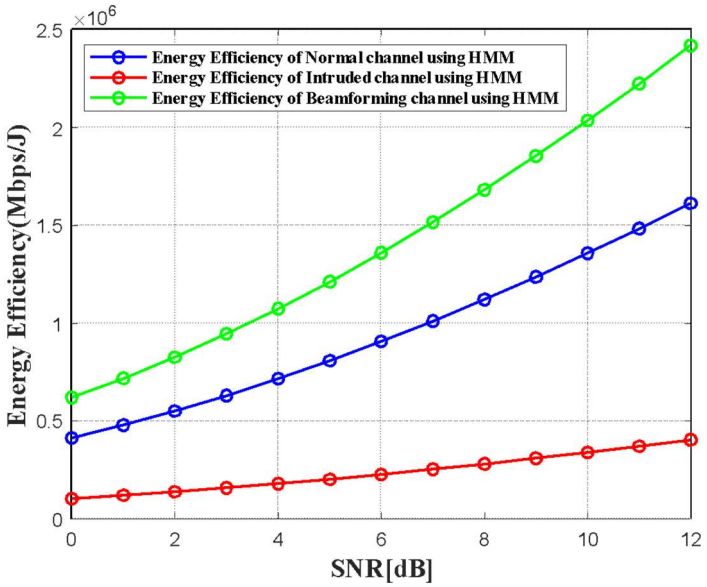

Figure 13. Comparison of energy efficiency and SNR using HMM.

The figure describes the energy efficiency analysis with SNR. The comparison has been made with the normal channel energy efficiency, energy efficiency of the channel after the attack or intrusion and the energy efficiency of the channel applied with the beamforming approach. The values in this process are measured in bps/J. By adapting the beamforming approach, we had an increased energy efficiency as compared to the energy efficiency of the normal channel and values are in **Table 8**.

Table 8. Values of energy efficiency using HMM.

S.no.	Number of iterations	Different channels	Maximum energy efficiency
1	100	Normal channel	1.53 Mbps/J
2	100	Intruded channel	0.47 Mbps/J
3	100	Beamformed channel	2.48 Mbps/J

4.4. Secrecy rate

Figure 14 clearly describes the secrecy rate with SNR. Secrecy rate is actually a measure that how secretly the data is transmitted over a channel. Secrecy rate is calculated with the channel capacity of the channel before and after the intrusion. The comparison of the values is depicted in this figure for the secrecy rate analysis of the normal channel and the secrecy rate analysis of the beamformed channel with respect to the diversity approach. Hence from the above results gained from the comparison, it can be concluded that by adopting the beamforming approach increases the secrecy rate of the channel and hence diversity is the phenomena which is the main component for the high secrecy rate in the channel.

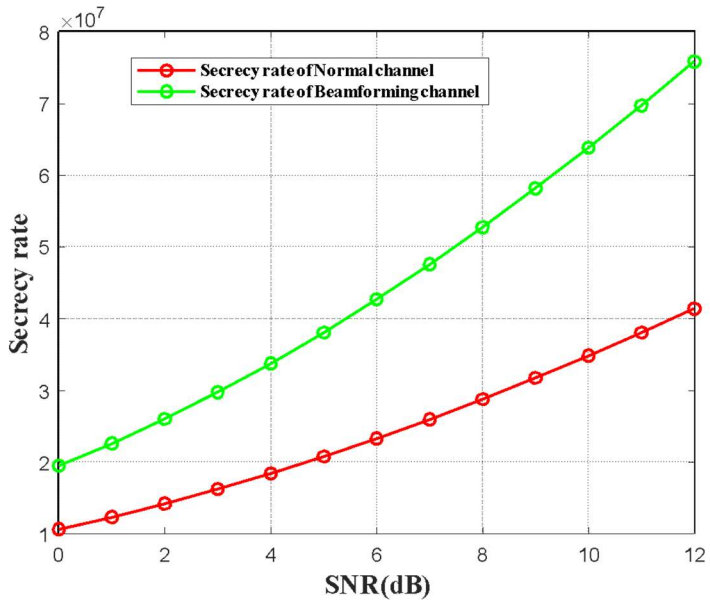

Figure 14. Comparison of secrecy rate and SNR

Figure 15 clearly describes the secrecy rate with SNR using HMM. Secrecy rate is actually a measure of how secretly the data is transmitted over a channel. Secrecy rate is calculated with the channel capacity of the channel before and after the intrusion. The comparison of the values is depicted in this figure for the secrecy rate analysis of the normal channel and the secrecy rate analysis of the beamformed channel with respect to the diversity approach. Hence from the above results gained from the comparison, it can be concluded that by adopting the beamforming approach increases the secrecy rate of the channel and hence diversity is the phenomena which is the main component for the high secrecy rate in the channel.

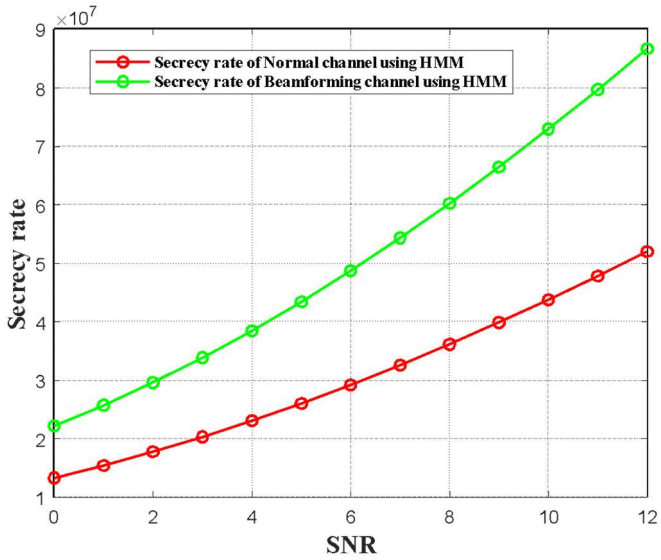

Figure 15. Comparison of secrecy rate and SNR using HMM.

4.5. Secrecy outage probability

Figure 16 describes the concept of secrecy outage probability and the comparison in the values of the theoretical concept proposed earlier and the values of the proposed scenario in this thesis. As known, there is a least value of channel capacity that decreases from that specific value, the probability of non-secure transmission of data is possible. Hence this phenomenon is defined as secrecy outage probability and for a secure communicative network, the SOP should be decreasing with SNR. Hence this figure clearly depicts the comparison between the SOP of the already stated theoretical scenario and the proposed scenario stated in this thesis with SNR. As this figure describes, the values of SOP of the proposed scenario in this thesis are lower as compared to the theoretical scenario which is hence required from this phenomenon.

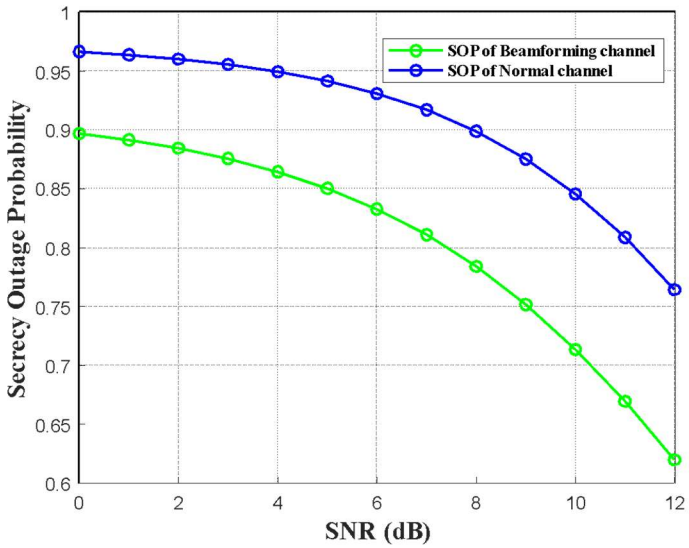

Figure 16. Comparison of secrecy outage probability and SNR.

Figure 17 describes the concept of Secrecy outage probability and the comparison in the values of the normal channel and beamforming channel using HMM

in this thesis. As known, there is a least value of channel capacity that decreases from that specific value, the probability of non-secure transmission of data is possible. Hence this phenomenon is defined as secrecy outage probability and for a secure communicative network, the SOP should be decreasing with SNR. Hence this figure clearly depicts the comparison between the SOP of the already stated theoretical scenario and the proposed scenario stated in this thesis with SNR. As this figure describes, the values of SOP of the proposed scenario in this thesis are lower as compared to the theoretical scenario which is hence required from this phenomenon.

In this paper, by using HMM with Beamforming approach a high secrecy rate has been achieved in order to avoid intrusion and wastage of resource blocks.

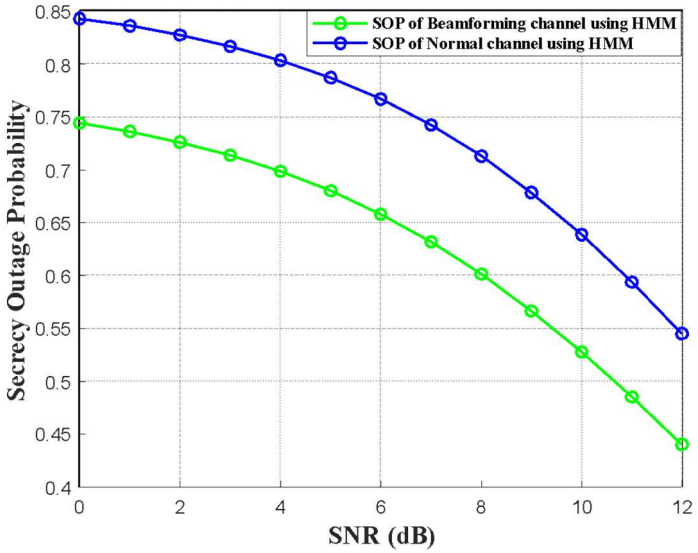

Figure 17. Comparison of secrecy outage probability and SNR using HMM.

From the results that are analyzed from the proposed concept, it is observed that in comparison to the existing scenario, a considerable improvement in channel capacity, spectral and energy efficiency and secrecy rate and decrease in secrecy outage probability obtained with the proposal made in this thesis. . Such high values of channel capacity, spectral and energy efficiency and decrement in secrecy outage probability are what actually are targeted by the 5G networks and are highly desirable to meet the rising subscriber's demands.

- Limitations

This research is limited by basic drawbacks of adaptive beamforming; the robustness is lost if there is a very small mismatch condition that arises in the array response vector. This mismatching in the array response vector practically arises when the characteristics of the true signal are different from that of the assumed ones.

5. Conclusion and future scope

As the number of subscribers are increasing, so are their demands for high data rates and secure communication. This thesis presented security issues in the 5G network. An extensive literature survey on the security scenario in D2D wireless communication network has been first received. We proposed to use adaptive resource allocation by using HMM with a diverse beamforming approach. We focus on using

no orthogonal resource sharing mode, as it is effective for enhancing spectral efficiency of the cellular networks. Addition to this beamforming approach is also impinged for the higher values of the parameters of a WCN. Architecture for adaptive resource allocation for allocating the resource blocks to all the users optimally, followed by a beamforming approach with respect to the diversity phenomena is proposed. A stochastic approach is espoused for prime resource allocation to the CUs in the network. Adaptive allocation of resource blocks is performed within the network on the root of the applications demanded by CUs (video, voice or data). And after the resource allocation, the concept of diversity in the beamforming approach is impinged in order to secure the transmission of data.

The proposed architecture and algorithm for resource allocation is based on Hidden Markov Model (HMM) followed by diversity in the beamforming approach primarily targeting channel capacity maximization, enhanced secrecy rate and reduction in Secrecy Outage Probability (SOP). It is an operative elucidation for overpowering the numerous open issues in D2D communication network for CUs. With the proposed methodology, resources are mutual between the two types of users (cellular user equipment and D2D user equipment) efficiently without any resource wastage.

Initially, enhancement in channel capacity is witnessed with the use of sector antennas at the BS (theoretical architecture). Furthermore, higher values of the channel capacity are achieved by the application of the proposed adaptive resource allocation algorithm, which is eventually based on the Hidden Markov Model. Addition to it, for higher values of secrecy rate and lower value of secrecy outage probability, beamforming approach w.r.t. diversity is an optimal solution. This proposed scheme is capable of adaptively distributing the RBs without wastage according to the application that has been demanded and for the secure transmission of the RBs from BS to the particular CUs. A comparative study for the different parameters of the network like channel capacity, spectral and energy efficiency, secrecy rate and secrecy outage probability has been done between the theoretical scheme and the proposed scheme for depicting the improved results. The main focus of the architecture remains optimal resource allocation so as to meet the subscribers demands for channel capacity in the most efficient and preferable manner for higher secrecy rate using beamforming approach. A channel capacity value of up to 102 Mbps is achievable with the proposed algorithms and high values are desirable for the next generation.

Since by the use of directive antennas we are able to direct the beam to the user which is under attack for the secure communication between the BS and the cellular users. As a result, this architecture can be used as a primal solution for the scenario which is under attack having the RBs allocated with larger size. In the 5G networks, dense deployment scenarios are supported, which results in Ultra Dense Networks (UDNs). These mentioned networks are highly prone to attacks due to large numbers of subscribers like jamming which is a big threat for the secure transmission of data. The proposed network architecture is, in the way, prone to eavesdroppers, jammers etc. Research on the security aspect of the cellular links in such networks is a very open field for research work. **Table 9** depicts the symbols used in paper.

Table 9. Representation of symbols.

S.no.	Representation of symbols	Meaning of symbols
1	$G_{d,cu(b)}$	Channel gain taken between the cellular users.
2	$I_{b,d(a)}$	The gain of interference link from the base station (BS) to a-th D2D pair.
3	$I_{d(a)cu(b)}$	The interference link gain from *a*-th D2D pairs receiver to its *b*-th cellular users.
4	$P_{d(a)}$, $P_{cu(b)}$	The transmitted power of the *a*-th D2D pair and *b*-th cellular users.
5	Y_r, Y_{re}	The received signal strengths at BS of cellular user and eavesdropper
6	$P_{cu(b)}$, P_{txe}	The transmission power from user and eves to BS.
7	H_{MN}, H_{MNe}	The impulse responses of the channel for user and eves.
8	S_{th}, S_{the}	The signal strength transmitted by user and eves.
9	σ_v	Noise variance
10	SnR	Signal-to-Noise Ratio with respect to cellular users
11	$P_{r,cu(b)}$	Received power from BS to CU
12	P_l	Path loss
13	$C_{Hm}{}'$	Channel Capacity of normal channel
14	$cu(b)$	The SINRs of *b*-th cellular user
15	Rs'	The reuse component of resource block of the cellular users with respect to D2D users.
16	P_B	The number of users and transmission powers of RBs
17	$sinr_a^{k,b}$	At the receiver the SINR of the *a*-th D2D pair which is sharing *k*-th RB of *b*-th user
18	α_t	The total interference that is encountered by the *a*-th D2D pair.
19	$P_a^{k(b)}$	At the receiver the power received by the *a*-th D2D pair which is sharing *k*-th RB of *b*-th user.
20	$h_a^{k(b)}$	At the receiver the channel coefficient of the a-th D2D pair which is sharing *k*-th RB of *b*-th user.
21	$Th_a^b(n)$	For *a*-th pair the achievable throughput with n iteration
22	$Th_d(n)$	For d pairs the total throughput for each iteration
23	SnR'	Signal-to-noise ratio with respect to Eavesdropper.
24	$P_{r,E}$	Received power from BS to eves.
25	BW	Resource block bandwidth
26	C_{HmE}'	Channel capacity of eves intruded channel
27	SRt	Secrecy rate
28	P_o	Secrecy outage probability
29	$R_{RT1}{}'$, $R_{RT2}{}'$ and $R_{RT3}{}'$	The code transmissions of data rates of U(1), U(2) and U(3)
30	$R_c{}'$	Threshold value of secrecy rate of a channel.
31	Y_{rb*}, Y_{rb*e}	The received signal strengths at BS of CU and Eavesdropper in the beamforming scenario.
32	$P_{cu(b)b*}$, P_{txb*e}	The transmission power from user and eves to BS in the beamforming scenario.
33	H_{Mb*}, H_{Mb*e}	The impulse responses of the channel for user and eves.

Table 9. (*Continued*).

S.no.	Representation of symbols	Meaning of symbols
34	S_{tb*}, S_{tb*e}	The signal strength transmitted by user and eves in the beamforming scenario
35	SnR''	Signal-to-Noise Ratio with respect to beamforming channel.
36	$P_{r,cu(b)b*}$	Received power from BS to CU in the beamforming channel.
37	$\|h_0\|$	Channel Coefficient of beamforming channel.
38	P_G	The antenna gain.
39	$C_{HBm}{}'$	Channel Capacity of normal channel in the beamforming approach
40	$cu(b)b*$	The SINR of the b-th cellular users is
41	$\sum_{b*} P_{cu(b)b*} W_{b*}^H g_{ibwb*}^I + \sigma_0$	The interference power from the BS to cu
42	$P_{r,E(b)}$	Received power from BS to eves in the beanforming scenario.
43	$C_{HBmE}{}'$	Channel capacity of eves intruded channel
44	δ	SNR of the beamforming channel
45	α	The path loss exponent
46	$r_{BS}^{-\alpha}, r_E^{-\alpha}$	The distance between base station and cellular user, distance between base station and eves in beamforming scenario

Conflict of interest: The author declares no conflict of interest.

References

1. Gupta A, Jha RK. A Survey of 5G Network: Architecture and Emerging Technologies. IEEE Access. 2015; 3: 1206-1232. doi: 10.1109/access.2015.2461602
2. Han C, Harrold T, Armour S, et al. Green radio: radio techniques to enable energy-efficient wireless networks. IEEE Communications Magazine. 2011; 49(6): 46-54. doi: 10.1109/mcom.2011.5783984
3. Asadi A, Wang Q, Mancuso V. A Survey on Device-to-Device Communication in Cellular Networks. IEEE Communications Surveys & Tutorials. 2014; 16(4): 1801-1819. doi: 10.1109/comst.2014.2319555
4. Technical specification group radio access network; evolved universal terrestrial radio access. Available online: https://www.freecalypso.org/pub/GSM/3GPP/archive/36_series/36.300/36300-b70.pdf (accessed on 26 July 2024).
5. Godara LC. Applications of antenna arrays to mobile communications. I. Performance improvement, feasibility, and system considerations. Proceedings of the IEEE. 1997; 85(7): 1031-1060. doi: 10.1109/5.611108
6. Gandotra P, Kumar Jha R, Jain S. A survey on device-to-device (D2D) communication: Architecture and security issues. Journal of Network and Computer Applications. 2017; 78: 9-29. doi: 10.1016/j.jnca.2016.11.002
7. Ma D, Tsudik G. Security and privacy in emerging wireless networks [Invited Paper]. IEEE Wireless Communications. 2010; 17(5): 12-21. doi: 10.1109/mwc.2010.5601953
8. Claussen H, Ho LTW, Pivit F. Effects of joint macrocell and residential picocell deployment on the network energy efficiency. In: Proceedings of the 2008 IEEE 19th International Symposium on Personal, Indoor and Mobile Radio Communications. pp. 1-6.
9. Derryberry RT, Gray SD, Ionescu DM, et al. Transmit diversity in 3G CDMA systems. IEEE Communications Magazine. 2002; 40(4): 68-75. doi: 10.1109/35.995853
10. Wang CX, Haider F, Gao X, et al. Cellular architecture and key technologies for 5G wireless communication networks. IEEE Communications Magazine. 2014; 52(2): 122-130. doi: 10.1109/mcom.2014.6736752

11. Nguyen VD, Duong TQ, Dobre OA, et al. Joint Information and Jamming Beamforming for Secrecy Rate Maximization in Cognitive Radio Networks. IEEE Transactions on Information Forensics and Security. 2016; 11(11): 2609-2623. doi: 10.1109/tifs.2016.2594131
12. Chopra G, Kumar Jha R, Jain S. A survey on ultra-dense network and emerging technologies: Security challenges and possible solutions. Journal of Network and Computer Applications. 2017; 95: 54-78. doi: 10.1016/j.jnca.2017.07.007
13. Alotaibi ER, Hamdi KA. Secrecy outage probability analysis for cooperative communication with relay selection under non-identical distribution. In: Proceedings of the 2016 IEEE Wireless Communications and Networking Conference.
14. Zhang Y, Ko Y, Woods R, et al. Defining Spatial Secrecy Outage Probability for Exposure Region-Based Beamforming. IEEE Transactions on Wireless Communications. 2017; 16(2): 900-912. doi: 10.1109/twc.2016.2633351
15. Yu B, Yang L, Ishii H. 3D beamforming for capacity improvement in macrocell-assisted small cell architecture. In: Proceedings of 2014 IEEE Global Communications Conference; 08–12 December 2014; Austin, TX, USA. 2014. pp. 4833-4838. doi: 10.1109/GLOCOM.2014.7037571
16. Dugad R, Desai UB. A Tutorial on Hidden Markov Models. 2000.