www.ijaceeonline.com ISSN: 2456 - 3935
International Journal of Advances in Computer and Electronics Engineering
Volume 6, Issue 10, October 2021, pp. 1 – 8

IoT-NOMA Physical Layer Security Under Untrusted Users and Secret Key-Capacity Limitation

Juhi Singh
Research Associate, Department of Electronics and communication,
GLA University, Mathura, India
Email: juhisi.94@gmail.com

Abstract: *Under same resources, PD-NOMA has characteristics to decode the messages of other paired users. And to achieve the privacy in communication for IoT is difficult now-a days, mostly employing technique for secure communication is cryptography. And for cryptography means to establish the communication between transceivers, pre-agreement is done and this is done using key BS is treated with untrusted users then the chances for threatening the security for communication increases between two transceivers, the key-length is defined by MI and there is limitation for MI under the specification of IEEE 802.15.4. So, to calculate the secret-key capacity under eavesdropper have some limitations. On the other hand, using legitimate user and eavesdropper in two-user NOMA, OP and SOP is going to derived within a cell. Also, explanation of SIC is mention by using 3 users.*

Keyword: *NOMA systems; IoT; Physical layer security; eavesdropper; secret-key capacity;*

1. INTRODUCTION

The For future communication, PLS and NOMA both are promising techniques for establishing fast and secure communications between devices [1]-[4]. To guarantee the secure and efficient wireless transmission, investigation is going-on to find the co-existence and optimization of the PLS in NOMA is focused under eavesdropper. Still have lack of studies and theories to achieve the optimal results in the presence of untrusted users in NOMA systems. Since, mobile network traffic is increases day-by-day which creates congestion and chances for security increases. To meet the need of such traffic, NOMA is considered one of the most promising technologies [1]. NOMA systems have many variations but the concept is same i.e., within same time and frequency multiple users are served. There are generally two types i.e., Power domain non-orthogonal multiple access [5],[6] and other one is code domain non-orthogonal multiple access [7]-[9] which provides better performance and spectral efficiency over OMA, OFDMA, TDMA and CDMA.

In this paper, PD-NOMA adopted in which super-position coding is done at transmitter side and successive interference cancellation (SIC)is done at receiver side [10]. For distinguishing the super-position coded signals at receiver, users at transmitter are ordered and according to their channel different power levels are allocated. This results to remove the interference the users can use SIC. As a outcome, to improve the performance of weak users in second time slot, strong users (near users) can work as a relay which helps re-sending the decoded information [11-14]. In different time slots, weak users can combine the received information using maximum ratio combining (MRC).

For wireless communication networks, to get a secure communication is a challenge because of security threats by eavesdropper as due to broadcast nature in transmitting the signals. There is issue of security in higher layers in OSI models. PLS technique is considered for next generation wireless networks. In [15], Wyner proposed PLS to improve networks security by cryptography techniques. Many systems have been studied for security of physical-layer such as multiple-input-multiple-output (MIMO) [16], cooperative relaying [11]-[13], energy harvesting [17], artificial –noise aided transmission [18] full-duplex [12],[13], cognitive radio [19],[20].

For NOMA-based networks, physical –layer security has considered. In [2], author investigated for single antenna in a 5G NOMA system for physical layer security. In [3], to enhance the PLS author proposed a scheme for full-duplex relaying i.e., joint NOMA and artificial-noise (AN) called Non-Orthogonal Multiple Access-Artificial Noise Full Duplex Relaying (NOMA-ANFDR). In [4], under two NOMA legitimate users, author proposed a scheme for multiple-input-single-output (MISO)i.e., secrecy beamforming (SBF) and this scheme is useful for improving the secrecy of information. Simultaneous Wireless Infor-

Cite this paper:
Juhi Singh, "IoT-NOMA Physical Layer Security Under Untrusted Users and Secret Key-Capacity Limitation", International Journal of Advances in Computer and Electronics Engineering, Vol. 6, No. 10, pp. 1-8, October 2021.

ISSN: 2456 - 3935
International Journal of Advances in Computer and Electronics Engineering
Volume 6, Issue 10, October 2021, pp. 1 – 8

mation and Power Transfer (SWIPT) is a scheme used for AN-cooperative jamming in a MISO-NOMA. In [22], author studied under QoS requirements i.e., power allocation process for maximizing the secrecy sum rate of NOMA system while in [23], author investigated power allocation and power capabilities in NOMA with SWIPT.

We study under two-users NOMA system with an eavesdropper and finding outage and secrecy performance. The purpose is to find the feasibility of outage optimal performance of the pair under secrecy outage-optical performance. For IoT devices, cryptographic protocols may not be sufficient due to security issue in higher levels of OSI model [24]. In recent years, some renewed effort is done for cryptographic protocols [25], [26],[27]

Between two transceivers encryption key may be promising direction for the observations of common channel. (Methods [28], [29] have been proposed using the theory of reciprocity for antennas and electromagnetic propagation along with bidirectional transmissions occur inside the coherence time) for communicating parties based on channel impulse response for agreeing to a key.

Between the observations of two radios, maximum size of a binary sequence that can be shared. For a variety of channels [30], [31], [32] theoretical work has been done in the past for calculating the upper bound of MI. Received signal strength indicator (RSSI) has been calculated over the past experimental works but they have to depend on FEC to correct errors and these errors are caused due to the inconsistencies between the two extracted sequences

2. COMPARISON BETWEEN NOMA AND OMA

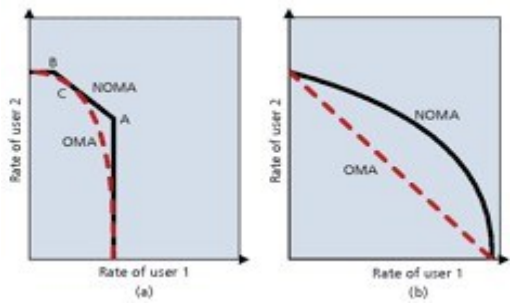


Figure 1 Channel capacity comparison of OMA and NOMA in an AWGN channel: a) uplink AWGN channel; b) downlink AWGN channel. [9]

OMA is a conventional and presently used technique in which multiple users are allowed to share radio resources in time, frequency and code domain orthogonally. Since due to the orthogonality there is no existence of interference means there is easy reception or separation of signals but to its hard sometimes to achieve high sum-rate.

Non-orthogonal Multiple Access is a recent technique which will the future of 5G and IoT networks in which high achievable rate can be get along with spectral efficiency also improved with the help of NOMA as compared to OMA.

In Fig (1a), from [9] author explains that without loss of generality, comparison of OMA and NOMA is done for multi-user capacity for Additive White Gaussian Noise (AWGN). At point C, Uplink NOMA achieves the upper bound in compare to OMA.

Fig (1b) shows that NOMA rate pairs is outside then OMA rate pairs. If Channel State Information (CSI) is known to the receiver, then NOMA is optimal while OMA is suboptimal in the presence of Inter-symbol Interference (ISI). Massive connectivity in non-orthogonal is the number of users that are supported. Through this way number of users supported by NOMA is more than that of OMA. In OMA, scheduling request has to be sent first by a user to the Base Station (BS) then transmission is done which produces latency in the transmission and reception of signals. But this problem must be resolved in 5G networks as massive number of users has to connect for that latency should be minimal, so that NOMA is considered to be the solution and also helpful in connecting the IoT devices.

The paper is organized in two manners. In I part, SOP and OP is derived in closed-form expression for physical layer security under eavesdropper for NOMA system. In another, to find the practical limit of the secret-key capacity for physical layer security. Finally, at last section concludes the paper.

Notations: Following are the notations used in this work that are $\Pr\{X\}$ is the probability of event X, $f_N(x)$, $F_N(x)$ are the probability density function (PDF) and cumulative distribution function (CDF) of the random variable N respectively ln(.) and $log_2(.)$ are the logarithm of the natural and 2 bases, respectively exp(.) is the exponential function. Finally, the $x \sim \mathcal{CN}(\mu, \sigma)$ x is the complex distributed with mean μ and variance σ.

3. SYSTEM MODEL

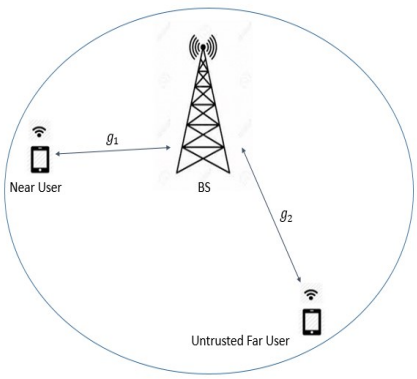


Figure 2 Two-user NOMA system with different clearance security

ISSN: 2456 - 3935
International Journal of Advances in Computer and Electronics Engineering
Volume 6, Issue 10, October 2021, pp. 1 – 8

In this paper, a cellular system is based on NOMA is considered with two users one is near user and another is untrusted user/eavesdropper as shown in Figure 1.

4. EXPRESSIONS AND ANALYSIS OF PERFORMANCE

In this section, closed form expression of the OP is derived and then SOP is derived for user U_1 then study the analytical derivation for securing the NOMA system.

A. Derivation of OP pair

Using Shannon's capacity [24] and assuming C_1^{th} and C_2^{th} are the threshold capacities of users U_1 and U_2. So, OP can be given by

$$OP_1 = 1 - Pr\{SINR_2^2 > \pi_2, SINR_2^1 > \pi_2, SINR_1^1 > \pi_1, \}$$

$$= 1 - Pr\{SINR_2^2 > \pi_2\} \times Pr\{SINR_2^1 > \pi_2, SINR_1^1 > \pi_1\}$$

$$= 1 - \Pr\{|g_2|^2 > \varphi_1\} Pr\{|g_1|^2 > max(\varphi_1, \varphi_2)\}$$

$$= 1 - Q_1 \times Q_2 \quad (6)$$

Where $\pi_i = 2^{\mathbb{C}_i^{th}}$ for i∈ {1,2}

$$\varphi_1 = \frac{\pi_2}{\rho(\alpha_2 - \pi_2\alpha_1)}$$

$$\varphi_2 = \frac{\pi_1}{\rho\alpha_1}$$

$$Q_1 = Pr\{|g_2|^2 > \varphi_1\}$$

$$= 1 - F_{|g_2|^2}(\varphi_1)$$

$$= \begin{cases} exp\left\{\frac{-\varphi_1}{\lambda_2}\right\}, & 0 < \alpha_1 < \frac{1}{1+\pi_2} \\ 0, & otherwise \end{cases} \quad (7)$$

$F_{|g_2|^2}\{x\}$ is the CDF of exponentially distributed random channel $|g_2|^2$ and λ_2 is the parameter of the distribution. There are two cases to derived Q_2.

Case 1: $\varphi_1 > \varphi_2$

For this $\alpha_1$need to be satisfied:

$$\alpha_1 > \frac{\pi_1}{\pi_1 + \pi_2 + \pi_1\pi_2}$$

So, Q_2=Pr$\{|g_1|^2 > \varphi_1\}$

$$= 1 - F_{|g_1|^2}(\varphi_1)$$

$$= \begin{cases} exp\left(\frac{-\varphi_1}{\lambda_1}\right), & \frac{\pi_1}{\pi_1+\pi_2+\pi_1\pi_2} < \alpha_1 < \frac{1}{1+\pi_2} \\ 0, & otherwise \end{cases} \quad (8)$$

Where $F_{|g_1|^2}\{x\}$ is CDF of exponentially distributed random channel $|g_1|^2$and λ_1 is the parameter of the distribution.

Case 2: $\varphi_1 < \varphi_2$

For this $\alpha_1 < \frac{\pi_1}{\pi_1+\pi_2+\pi_1\pi_2}$

So Q_2=Pr$\{|g_1|^2 > \varphi_2\}$

$$= 1 - F_{|g_1|^2}(\varphi_2)$$

$$= \begin{cases} exp\left(\frac{-\varphi_2}{\lambda_1}\right), & 0 < \alpha_1 < \frac{\pi_1}{\pi_1+\pi_2+\pi_1\pi_2} \\ 0, & otherwise \end{cases} \quad (9)$$

On substituting equations (7),(8) and (9) in (6) we get

$$OP_1 \begin{cases} 1 - f(\alpha)y_1(\alpha), & \frac{\pi_1}{\pi_1+\pi_2+\pi_1\pi_2} < \alpha_1 < \frac{1}{1+\pi_2} \\ 1 - f(\alpha)y_2(\alpha), & 0 < \alpha_1 < \frac{\pi_1}{\pi_1+\pi_2+\pi_1\pi_2} \end{cases} \quad (10)$$

Where

$$f(\alpha) = exp\left\{\frac{-\pi_2}{\rho\lambda_2}\left(\frac{1}{1-\alpha_1(1+\pi_2)}\right)\right\} \quad (11)$$

$$y_1(\alpha) = exp\left\{\frac{-\pi_2}{\rho\lambda_1}\left(\frac{1}{1-\alpha_1(1+\pi_2)}\right)\right\} \quad (12)$$

$$y_2(\alpha) = exp\left\{\frac{-\pi_1}{\rho\lambda_1\alpha_1}\right\} \quad (13)$$

Derivation of SOP of U_1

Using Shannon's capacity formula [24], secrecy rate of user U_1 can be given by

$$\mathbb{C}_1 = I_1^1 - I_1^2$$

$$I_1^1 = log_2(1 + SINR_1^1) \quad (14)$$

$$I_1^2 = log_2(1 + SINR_1^2) \quad (15)$$

Where $\mathbb{C}_1$is the non-negative secrecy capacity of U_1. Given the secrecy capacity in [14, the SOP of U_1 can be given by

$$SOP_1 = Pr\{\mathbb{C}_1 < R_{SU}\}$$

$$= Pr\left\{\frac{1 + SINR_1^1}{1 + SINR_1^2} < \pi_s\right\}$$

$$= Pr\{|g_1|^2 < \pi_s|g_2|^2 + \mathcal{X}\}$$

$$= 1 - \int_{x=0}^{\infty} F_{|g_1|^2}(\pi_s|g_2|^2 + \mathcal{X})\, f_{|g_2|^2}(z)dz$$

ISSN: 2456 - 3935
International Journal of Advances in Computer and Electronics Engineering
Volume 6, Issue 10, October 2021, pp. 1 – 8

$$= 1 - \int_{z=0}^{\infty} \left[1 - exp\left\{\frac{-\pi_s|g_2|^2+\mathcal{X}}{\lambda_1}\right\}\right] \frac{e^{-\frac{z}{\lambda_2}}}{\lambda_2} \, dz$$

$$= 1 - \beta e^{\frac{-\mathcal{X}}{\lambda_1}} \quad (16)$$

Where R_{SU} is the secrecy target rate of the user U_1

$\pi_s = 2^{R_{SU}}$, $f_{|g_2|^2}(z)$ is the PDF of $|g_2|^2$,

$$\beta = \frac{\lambda_1}{\lambda_1 + \lambda_2 \pi_s}$$

$$\mathcal{X} = \frac{\pi_s - 1}{\alpha\rho}$$

B. Obtaining Optimal OP under SOP constraint

To achieve maximum allowable SOP threshold, we need to find the minimum power allocation factor α_{SOP}. This threshold value of the power allocation factor can be found by making equation (5c) at $SOP_1 = \varepsilon$

$$\alpha_{SOP} = \frac{\pi_s - 1}{\lambda_1 \rho ln\left(\frac{\beta}{1-\varepsilon}\right)} \quad (17)$$

Theorem stated below provides the feasibility condition for obtaining outage-optimal solution i.e.,

Theorem: Optimal OP of the NOMA pair under the SOP constraint in (5c) is feasible if and only if

$$0 < \alpha_{SOP} < \alpha^*$$

Proof: We need to investigate the monotonicity of the SOP of user U_1 in order to prove the above theorem Differentiating SOP w.r.t. α is given by

$$\frac{dSOP_1}{d\alpha} = \frac{-\lambda_1(\pi_s - 1)}{\rho\lambda_1\alpha^2(\lambda_1 + \lambda_2\pi_s)} e^{\frac{-(\pi_s-1)}{\rho\lambda_1\alpha}} \quad (18)$$

which is always less than zero. This shows that SOP of U_1 is monotonically decreasing function of α, which leads to the fact the α^* (optimal power allocation factor) must be greater then α in order to satisfy the secrecy constraint.

In other words, unless $0 < \alpha_{SOP} < \alpha^*$, we can't achieve outage-optimal and satisfy the SOP constraint.

C. Study of MI

It is important to quantify the size of the bit sequence that size of the bit sequence that between the two communicating parties MI is to be calculated. Some assumptions are made i.e., Eavesdropper 'E' can listen all communications between the authenticated parties that are Alice 'A' and Bob 'B' [15]. 'E' is completely passive, i.e., doesn't create jam in the medium at any time.

D(a). Key-capacity

Due to the knowledge of Y, Mutual Information I(X;Y) and X is the uncertainty

Since, I(X;Y)=H(X)-H(X/Y)=H(Y)-H(Y/X)

Where

$$H(X/Y) = -\sum_{y\epsilon Y}\sum_{x\epsilon X} p(x,y) log_2\left(\frac{x}{y}\right) \quad (19)$$

$$H(Y/X) = -\sum_{y\epsilon Y}\sum_{x\epsilon X} p(x,y) log_2\left(\frac{y}{x}\right) \quad (20)$$

Measurements of RSSI so that every packet exchanged are the random variables. X is sequence of RSSI values measured by A whereas Y for B. If X and Y are independent and uncorrelated, I(X;Y) becomes zero. From (19), due to the entropy of two sources MI is upper-bounded. Hence, H(X) and H(Y) have higher potential that can lead to higher-key capacities.

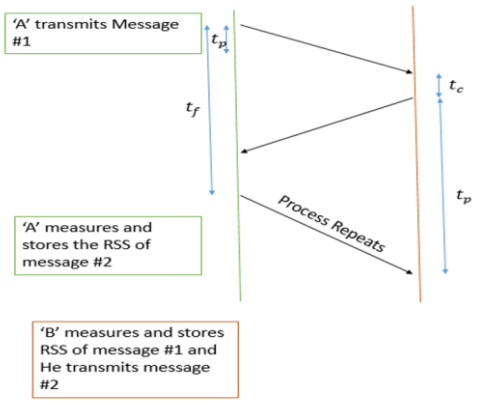


Figure 3 Illustration of RSSI Methodology

D(b). Secret Key-Capacity

Upper bound might not be equal to I(X;Y) if 'A' and 'B' wish to agree to a key that is kept secret from an eavesdropper. Assume that 'E' observes the transmitted packets and logs their RSSI values. $z_x \epsilon Z_X$ and $z_y \epsilon Z_Y$ respectively.

Secret key capacity is upper-bounded by

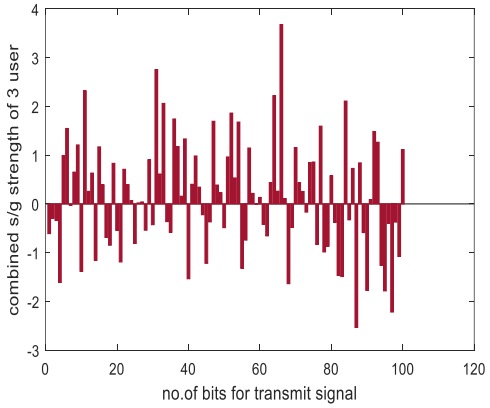
$$K(X;Y\| Z) =$$
$$\min\left[I(X;Y), I(X;Y/Z_X), I(X;Y/Z_Y), I(X;Y/Z_X Z_Y)\right.$$

$I(X;Y/Z)$ can be smaller or bigger than I(X;Y). It is also possible that 'E' can fail to capture some exchanged packets in case of packet loss.

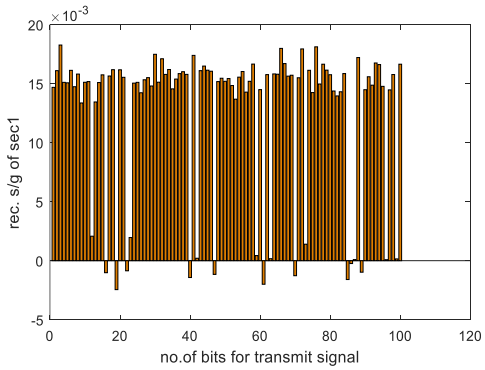
ISSN: 2456 - 3935
International Journal of Advances in Computer and Electronics Engineering
Volume 6, Issue 10, October 2021, pp. 1 – 8

5. TYPES OF NOMA

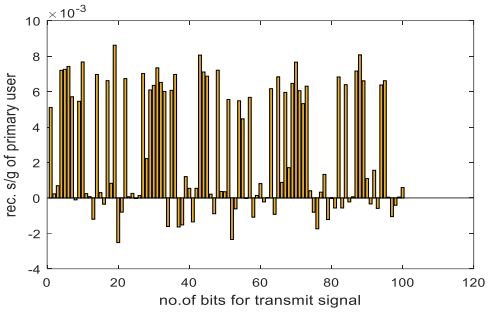
NOMA is of two types: one is Power Domain NOMA(PD-NOMA) and another is Code Domain NOMA (CD-NOMA). In PD-NOMA, power is distributed according to the channel conditions among the different users to increase the performance of the system. In CD-NOMA different users are assigned with different codes and then multiplexed with time-frequency resources [7-9]. NOMA will be useful to improve the spectral efficiency [9]. In PD-NOMA, signals added linearly from different multiplexed users and at receiver signals are extracted through the process of Successive Interference Cancellation (SIC). To understand the method of SIC, let's take an example with 3 users

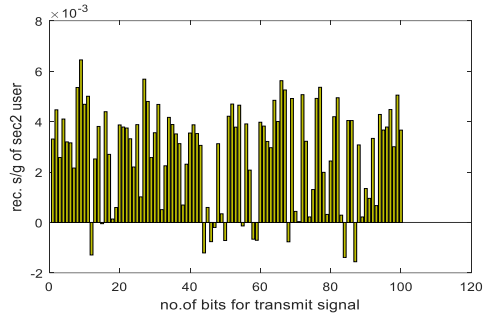


Combined Signal strength of 3 users i.e., primary user, secondary user1 (farthest user from base station) and secondary user2 (nearest user at base station) at transmitter which is send to the receiver. Using SIC, which states that far user (weak user) should provide power strength so that signal can withstand during fading or multipath loss.



Above result show that farthest user has provided highest power strength which is extracted first then it is subtracted from combined signal strength to extract other users signal strength shown below





6. PHYSICAL LAYER ASPECTS [34]

There are physical layer techniques for IoT work as wireless network. As physical layer for IoT has the standards like IEEE 802.15.4, IEEE 802.15.6, Bluetooth Low Energy (BLE), EPCgobal, LTE-A, Z-Wave, 6LowPAN and NFC. Following describes the physical layer techniques for wireless IoT.

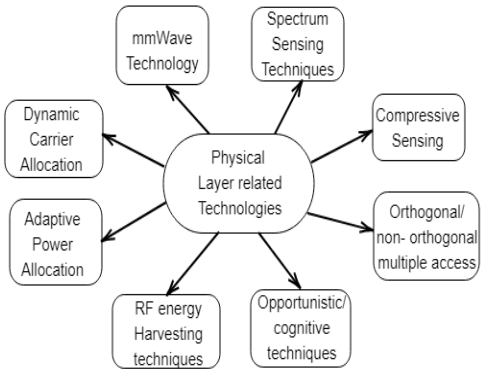


Figure 3Physical Layer Technique for wireless IoT

A. IoT in Wireless Sensor Networks (WSNs)

WSNs technique using physical layer are designed for the purpose of gaining high diversity, to maximize energy efficiency and also reducing the computational time. For WSNs, research aspects are categorized as:

- Requirement of transmitter-receiver design to better energy efficiency
- Low complexity data techniques

ISSN: 2456 - 3935
International Journal of Advances in Computer and Electronics Engineering
Volume 6, Issue 10, October 2021, pp. 1 – 8

Sensory environment is required for short distance communication like indoor communication. For such purpose energy consumption is the main issue for research. Along with this low energy consumption, sensor also captures good quality of information for a particular activity

B. IoT in Machine Type Communications (MTCs)

About 100 times will be the number of future wireless networks then current wireless networks. Wearable devices, Machine type communications/ device-to-device/ Vehicle-to-vehicle and wireless sensors are the parts of such scheme. Direct communication is done through these applications without transmitting any data to the base stations that helps to improve spectrum and energy efficiency. IEEE 802.11p standards are used for mostly MTCs which allows multiple access.

C. IoT in Satellite Communication

Satellite communication is used to cover large number of sectors as it provides broadband services over a wide range like marine, land mobile, aeronautics, transport, military, disaster relief etc. Smart grid, environmental monitoring and emergency management are connected with IoT for satellite communication. For such scenario, Low Earth Orbit (LEO) is used for control and automation. As we know that characteristics of satellite depends on weather forecasting like rains and storm due to which performance of satellite rigorously affected. So, to resolve such issues, power allocation with multi-carrier is properly investigated.

D.IoT in LTE-Advanced/5G networks

There is a need of Spectrum efficiency, energy efficiency and connectivity with low latency as there is rapidly increase in applications for IoT and 5G networks to improve the QoS to meet the needs of users. For that physical layer and MAC layer has to be optimized according to the user needs. For that there are many techniques that enabled IoT utilization such as millimeter wave(mmWave) technology which uses Bandwidth around 10-13 GHz in E-band. mmWave systems works in massive antenna array technologies like massive Multiple Input Multiple Output (MIMO) because beamforming and multiple access strategies are the performance parameters. Many researchers work on hybrid analog-digital beamforming and multiple access like NOMA

OFDM has many advantages as compared to TDMA, FDMA and CDMA. Combination of CDMA and OFDM technology are used for multiuser systems such as LTE-A, intercell-interference etc. OFDM has one of the major disadvantages that when block length is large then it has high PAPR. To remove this problem, good quality of power amplifier is needed. High PAPR results in degradation of Bit error rate performance.

There is lack of frequency spectrum for wireless transmission for supporting number of devices. Nyquist transmission is the current transmission approach where one symbol is transmitted per symbol duration. Future research 5G transmission networks contain more symbols that is more information in a duration. There may be the chances of Nyquist rate may be changes that is more Nyquist Rate is required.

7. PERFORMANCE EVALUATION

In this segment under different settings, we evaluate the correctness of analytical proposed scheme. Setup is same as previously described in system model Base station (BS) having the radius of about 1km and BS is deployed at the center of the cell that we have assumed. Small-scale fading and path loss effect are also there with respect to distance that the system suffers. Let assume the mean value 1 for small-scale fading that follows exponential distribution. Gaussian distribution is considered for all the noise present in the channel. Let consider the following:

$$\alpha(Path\ Loss\ Exponent) = 2$$

$$PL_o(Path\ Loss\ Constant) = 1$$

$$BW_{normalized} = 1Hz$$

From Figure 3, SOP of Trusted User is a decreasing function with respect to SNR whereas SNR increases as the distance of untrusted user increases so that signal strength of trusted increases. Moreover, in a high SNR regime in the curve shows that outage analysis converges to the true outage probability.

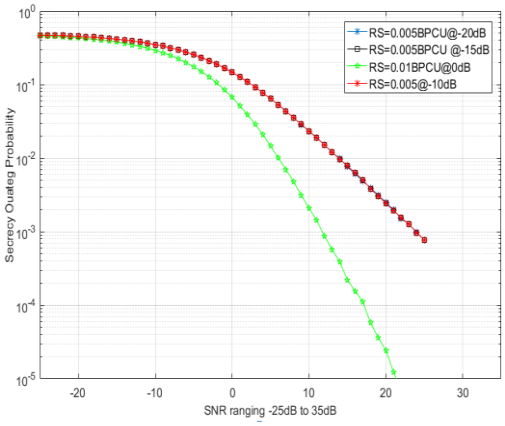


Figure 4 Secrecy Outage Probability of User1 with respect to SNR ranges from-25dB to 30dB and target secrecy rate (R_s)in terms of Bits Per Channel Use (BPCU)

In Figure 4 shows the analysis of performance depends on the positions of users. Here, the curve shows different position of trusted user with respect to BS and power allocation factor is depends on their position. The concept of power allocation is that to provide the strength of the trusted user when their signal strength

ISSN: 2456 - 3935
International Journal of Advances in Computer and Electronics Engineering
Volume 6, Issue 10, October 2021, pp. 1 – 8

is weak. When it is near to BS it requires less power when it is far away it requires the power to boost the signal strength. Result shows that trusted user with different distances marked as UE1, UE2, UE3 and UE4 which shows that when it is farthest from BS power allocation increases (UE1) as when it near to BS power allocation factor decreases (UE4).

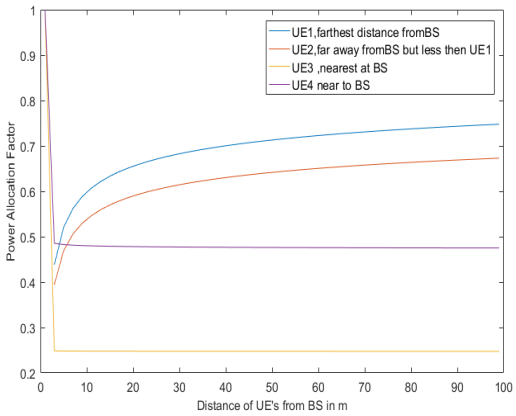


Figure 5 Adjustment of Power allocation factor according to distances of trusted and untrusted users

8. CHALLENGES & FUTURE DIRECTION

At physical layer, following are the challenges and future recommendations for IoT-NOMA

Requirement of Low-cost Transceiver which is energy efficient: Since to establish a IoT-NOMA network a large amount of component is need to be fabricated to make cost effective. Mostly are operated with battery and also located at remote area. So, these devices need to be fabricated in a miniaturized way. This will include cost challenges.

Imperfections of Hardware should be removed: non-orthogonal multiple access is the transmission scheme for IoT enabled devices for that receiver must have the property of interference cancellation. This is done when interference channel is accurately recognized along with covariance matrix. For low-cost devices Analog-to-Digital Converter (ADC) is required. There is a challenge for NOMA that is the designing with low resolution ADCs.

Compacting of Signal Processing for massive IoT systems: Since there is a requirement of high-rate ADC for that Nyquist Sampling is not realizable for the utilization of widely spread spectrum. There is a challenge of utilization of frequency, sparsity and time for IoT based systems also fading arises due to multipath environment for that signal processing with compactness is required. It also helps in sensing efficiently and channel estimation techniques.

Managing the Spectrum for wireless IoT: A highly reliable and scalable available radio spectrum is required for future IoT devices. Existing spectrum allocation technique is based on orthogonalization which is not suitable for future needs. A dynamic and non-orthogonal spectrum allocation policies are the solutions for future needs. There may be the chances of utilization of microwave and mmWave carrier frequency bands. To take advantage of dual band connectivity is one of the benefits of both microwave and mmWave frequency bands.

End-to-end system reliability using cross layer design: MAC layer and network layers' protocols are collectively used in physical layer for designing the end-to-end reliable communication systems. In case of designing MAC layer there is a need of synchronization, reliability and resource utilization efficiency and that challenge is created in case of duty cycle. In terms of delay and throughput for network layer, dynamic duty cycling has a considerable impact for end-to-end performance.

9. CONCLUSIONS

Successfully SOP and OP in closed-form expression is derived under untrusted users for physical-layer security. On the basis of analytical performance, an investigation is done. Theoretical results are verified by simulated results.

On the other hand, research shows that here is some conclusion that key-capacity is defined and characterized by MI between the observation of the two communicating parties after calculating the values of RSSI by putting different values of entropies. and this is happened due to extracting a shared bit sequence through observations of wireless medium is a promising direction.

REFERENCES

[1] Y. Saito, A. Benjebbour, Y. Kishiyama and T. Nakamura, "System-level performance evaluation of downlink non-orthogonal multiple access (NOMA)", *Proc. IEEE PIMRC*, pp. 611-615, June 2013.

[2] Y. Liu, Z. Qin, M. Elkashlan, Y. Gao and L. Hanzo, "Enhancing the Physical Layer Security of Non-Orthogonal Multiple Access in Large-Scale Networks", *IEEE Trans. Wirel. Commun.*, vol. 16, no. 3, pp. 1656-1672, March 2017.

[3] Y. Feng, Z. Yang and S. Yan, "Non-orthogonal multiple access and artificial-noise aided secure transmission in FD relay networks", *Proc. IEEE GLOBECOM Wkshps*, pp. 1-6, Dec 2017.

[4] L. Lv, Z. Ding, Q. Ni and J. Chen, "Secure MISO-NOMA transmission with artificial noise", *IEEE Trans. on Vehic. Tech.*, pp. 1-1, 2018.

[5] Z. Chen, Z. Ding, X. Dai and R. Zhang, "An optimization perspective of the superiority of NOMA compared to conventional OMA", *IEEE Trans. Signal Process.*, vol. 65, no. 19, pp. 5191-5202, Oct 2017

ISSN: 2456 - 3935
International Journal of Advances in Computer and Electronics Engineering
Volume 6, Issue 10, October 2021, pp. 1 – 8

[6] A. Li, Y. Lan, X. Chen and H. Jiang, "Non-orthogonal multiple access (NOMA) for future downlink radio access of 5G", *China Communications*, vol. 12, pp. 28-37, Dec 2015.

[7] H. Nikopour and H. Baligh, "Sparse code multiple access", *Proc. IEEE PIMRC*, pp. 332-336, Sept 2013.

[8] M. Moltafet, N. M. Yamchi, M. R. Javan and P. Azmi, "Comparison study between PD-NOMA and SCMA", *IEEE Trans. Veh. Technol*, vol. 67, no. 2, pp. 1830-1834, Feb 2018.

[9] L. Dai, B. Wang, Y. Yuan, S. Han, C. 1. I and Z. Wang, "Non-orthogonal multiple access for 5G: solutions challenges opportunities and future research trends", *IEEE Commun. Mag.*, vol. 53, no. 9, pp. 74-81, Sept 2015.

[10] N. Otao, Y. Kishiyama and K. Higuchi, "Performance of nonorthogonal access with SIC in cellular downlink using proportional fair-based resource allocation", *Proc. ISWCS*, pp. 476-480, Aug 2012.

[11] Y. Zou, X. Wang and W. Shen, "Optimal Relay Selection for Physical-Layer Security in Cooperative Wireless Networks", *IEEE J. Sel. A. Commun.*, vol. 31, no. 10, pp. 2099-2111, October 2013.

[12] L. Elsaid, L. Jiménez-Rodríguez, N. H. Tran, S. Shetty and S. Sastry, "Secrecy rates and optimal power allocation for full-duplex decode-and-forward relay wire-tap channels", *IEEE Access*, vol. 5, pp. 10469-10477, 2017.

[13] C. Dang, L. Jiménez-Rodríguez, N. H. Tran, S. Shetty and S. Sastry, "On secrecy rate and optimal power allocation of the full-duplex amplify-and-forward relay wire-tap channel", *IEEE Trans. on Vehic. Tech.*, vol. 66, no. 5, pp. 3887-3899, May 2017.

[14] B. M. Eihalawany, R. Ruby, T. Riihonen and K. Wu, "Performance of cooperative NOMA systems under passive eavesdropping", *Proc. IEEE GLOBECOM*, pp. 1-6, Dec 2018.

[15] A. D. Wyner, "The wire-tap channel", *The Bell System Technical Journal*, vol. 54, no. 8, pp. 1355-1387, Oct 1975.

[16] N. Yang, H. A. Suraweera, I. B. Collings and C. Yuen, "Physical Layer Security of TAS/MRC With Antenna Correlation", *IEEE Trans. Inform. Forensics and Security* , vol. 8, no. 1, pp. 254-259, Jan 2013.

[17] M. Zhang and Y. Liu, "Energy Harvesting for Physical-Layer Security in OFDMA Networks", *IEEE Trans. Inform.n Forensics and Security*, vol. 11, no. 1, pp. 154-162, Jan 2016.

[18] D. Tubail, M. EI-Absi, S. S. Ikki, W. Mesbah and T. Kaiser, "Artificial noise-based physical-layer security in interference alignment multipair two-way relaying networks", *IEEE Access*, vol. 6, pp. 19073-19085, 2018.

[19] Y. Zou, X. Wang and W. Shen, "Physical-Layer Security with Multiuser Scheduling in Cognitive Radio Networks", *IEEE Trans. Commun.*, vol. 61, no. 12, pp. 5103-5113, December 2013.

[20] Y. Jiang, J. Ouyang and Y. Zou, "Secrecy energy efficiency optimization for artificial noise aided physical-layer security in cognitive radio networks", *Proc. IEEE ITU K*, pp. 1-6, Nov 2017.

[21] F. Zhou, Z. Chu, H. Sun, R. Q. Hu and L. Hanzo, "Artificial noise aided secure cognitive beamforming for cooperative miso-noma using swipt", *IEEE J. Sel. A. Commun.*, pp. 1-1, 2018.

[22] Y. Zhang, H. M. Wang, Q. Yang and Z. Ding, "Secrecy sum rate maximization in non-orthogonal multiple access", *IEEE Commun. Let.*, vol. 20, no. 5, pp. 930-933, May 2016.

[23] G. He, L. Li, X. Li, W. Chen, L. L. Yang and Z. Han, "Secrecy sum rate maximization in noma systems with wireless information and power transfer", *Proc. WCSP*, pp. 1-6, Oct 2017.

[24] D. Tse and P. Viswanath, Fundamentals of wireless communication, Cambridge University Press, 2005.

[25] W. Diffie and M. E. Hellman, "New directions in cryptography,"Information Theory, IEEE Transactions on, vol. 22, no. 6, pp. 644–654,1976

[26] A. F. Skarmeta, J. L. Hernandez-Ramos, and M. Moreno, "A decentralized approach for security and privacy challenges in the internet of things," in Internet of Things (WF-IoT), 2014 IEEE World Forum on.IEEE, 2014, pp. 67–72.

[27] M. Abomhara and G. M. Koien, "Security and privacy in the internet of things: Current status and open issues," in Privacy and Security inMobile Systems (PRISMS), 2014 International Conference on. IEEE,2014, pp. 1–8.

[28] C. Ye and P. Narayan, "Secret key and private key constructions for simple multiterminal source models," Information Theory, IEEETransactions on, vol. 58, no. 2, pp. 639–651, 2012.

[29] J. Muramatsu, K. Yoshimura, P. Davis, A. Uchida, and T. Harayama,"Secret-key distribution based on bounded observability," Proceedings of the IEEE, vol. 103, no. 10, pp. 1762–1780, 2015.

[30] A. A. Hassan, W. E. Stark, J. E. Hershey, and S. Chennakeshu, "Cryptographic key agreement for mobile radio," Digital Signal Processing, vol. 6, no. 4, pp. 207–212, 1996.

[31] R. Wilson, D. Tse, and R. A. Scholtz, "Channel identification: Secret sharing using reciprocity in ultrawideband channels," Information Forensics and Security, IEEE Transactions on, vol. 2, no. 3, pp. 364–375,2007.

[32] R. Ahlswede and I. Csisz´ar, "Common randomness in information theory and cryptography. part i: secret sharing," IEEE Transactions on Information Theory, vol. 39, no. 4, 1993.

[33] R. Ahlswede and I. Csisz´ar, "Common randomness in information theory and cryptography. ii. cr capacity," Information Theory, IEEE Transactions on, vol. 44, no. 1, pp. 225–240, 1998.

[34] Shree Krishna Sharma, Tadilo Endeshaw Bogale, Symeon Chatzinotas, Xianbin Wang and Long Bao Le, "Physical Layer Aspects of Wireless IoT" 978-1-5090-2061-4/16/$31.00 ©2016 IEEE.

Authors Biography

Juhi Singh, is a Research Associate at GLA university Mathura, Department of ECE She completed B.Tech from F.E.T. Agra college and M.Tech from GLA university. Her research interest in wireless communication like 5G, NOMA, MIMO, OFDM, Cognitive Radio.

Cite this paper:

Juhi Singh, "IoT-NOMA Physical Layer Security Under Untrusted Users and Secret Key-Capacity Limitation", International Journal of Advances in Computer and Electronics Engineering, Vol. 6, No. 10, pp. 1-8, October 2021.