Secrecy Rate Maximization in Virtual-MIMO Enabled SWIPT for 5G centric IoT Applications

Ankita Jaiswal, Sushil Kumar, *Senior Member IEEE*, Omprakash Kaiwartya, *Senior Member IEEE*, Neeraj Kumar, *Senior Member IEEE*, Houbing Song, *Fellow IEEE*, Jaime Lloret, *Senior Member IEEE*

***Abstract*- In 5G centric sensors-enabled Internet of Things (IoT) applications, Virtual Multiple-Input Multiple-Output (V-MIMO) technique has witnessed significant attention as physical layer security enabler. In IoT, physical layer security is potential due to the vulnerability of wireless broadcasting in low computation capability and limited power source of the sensor nodes. In this regard, this paper presents a secure and energy efficient V-MIMO enabled simultaneous wireless information and power transfer (SWIPT) framework. The security framework uses beamforming and cooperative jamming signal to maximize the secrecy rate of the IoT systems. An optimization problem is formulated by collectively optimizing the beamforming vector, power splitting ratio and time switching ratio. Since the maximization problem is non-convex, to find solution of the problem an iterative algorithm is presented, which inherently uses the penalty function to find the solution. It is evident from simulation results that the secrecy rate optimization of the proposed framework is better as compared to the state-of-the-art techniques considering various metrics.**

***Index Terms*–Secrecy rate, Beamforming, 5G, Internet of Things, Wireless sensor networks**

I. Introduction

In 5G centric IoT applications, wireless communication system uses low-powered sensor nodes for data transmission with higher data rate and spectrum efficiency [1]. The broadcast nature of wireless communication leads hacking, modification and eavesdropping in data. In order to ensure the safety of the transmitted signals, increasing the operation time of sensors, lowering the energy consumption rate and improving the reliability of transmitted signals; physical layer security (PLS) is significant [2]. The virtual multiple-input multiple-output (V-MIMO), beamforming, and simultaneous wireless information and power transfer (SWIPT) are potential technologies for PLS. In V-MIMO, number of neighboring sensor nodes are brought together as cluster to operate cooperatively for data transmission and reception. It virtually converts single antenna into multiple antenna system to increase spectral efficiency through space multiplexing and link reliability through space diversity for 5G centric IoT [3].

A. Jaiswal and S. Kumar are with the School of Computer and Systems Sciences, Jawaharlal Nehru University, Delhi, 110067, India. Email:ankita79_scs@jnu.ac.in, skdohare@mail.jnu.ac.in

N. Kumar is with the Dept. of Computer Science & Eng., Thapar Institute of Engineering & Technology, Patiala, and School of Computer Science, University of Petroleum and Energy Studies, Dehradun, India. E-mail: neeraj.kumar@thapar.edu

O. Kaiwartya is with the Department of Computer Science, Nottingham Trent University, NG11 8NS, UK. E-mail: Omprakash.kaiwartya@ntu.ac.uk

H. Song is with the Dept. of Electrical Engineering and Computer Science, Embry-Riddle Aeronautical University, Florida, 32114 USA. Email: SONGH4@erau.edu

J. Lloret is with the University at Politecnica de Valencia, 46022, Valencia, Spain, Email: jlloret@dcom.upv.es

In SWIPT technique for radio frequency (RF) signal transmission, sensors are able to harvest energy through RF energy harvesting (EH) circuit and receive information from information decoding (ID) circuit simultaneously in time switching (TS) or power splitting (PS) mode [4]. Further, considering broadcast nature of the wireless communication in IoT system, transmitted information is exposed to the possibility of being wiretapped by the eavesdroppers. Cryptographic encryption at application layer is one of the most pragmatic approaches to resolve the problem of security for transmitted signals. Nevertheless, cryptographic methods are not suitable in low-powered and computationally constrained sensors-enabled IoT environment. Moreover, eavesdroppers have high computational power and thus, could possibly decrypt the encrypted information. Towards this end, PLS technique has the potential to address the security challenges for 5G centric sensors-enabled IoT [5]. It has been popularized to deliver secure communication channel in order to achieve significant secrecy rate[1] in spite of the higher computing power of eavesdroppers.

The beamforming is another PLS technique which focuses on the transmission of signals in a narrow direction only towards the authorized receiver [6]. It improves signal-to-interference-plus-noise ratio (SINR) and information rate at the receiving node by reducing the interference and multipath fading. Cooperative jamming signal or artificial noise is added by authorized receiver in the network to decrease the SINR level or cofounding the signals received by the eavesdroppers. It also provides guarantee to secure the information even if the condition of the channel between the transmitting sensor and the authorized receiving sensor is worse than that of the eavesdropper [7]. The non-orthogonal multiple access is also considered to provide high spectral efficiency and massive connectivity in multiuser environment using same frequency band simultaneously. However, limitation of non-orthogonal technique including higher complexity at receiver side for successive interference cancellation, considerable amount of channel gain difference is required to distinguish between strong and weak signal in cluster-based V-MIMO enabled SWIPT [8]. Most of the initial works on PLS are based on multiple antennas for applying MIMO in wireless communication. V-MIMO data transmission technique has been utilized to make the network more energy efficient. However, multiple signals transmission in V-MIMO enhances the possibility of snooping and wiretapping as no security measures are considered. Similar security concern has been addressed by symmetric key cryptography and cooperating jamming signals [9]. The cryptography requires higher computational power, energy and costly in key distribution. Here, EH scheme is not considered to compensate the higher energy consumption in the constrained IoT environment [10].

[1]The secrecy rate is defined as the difference between the data rate of main channel and the intercepted channel at receiver node

5G IoT network must address these challenges related to energy efficiency and security centric reliability. These challenges can be better addressed using V-MIMO enabled SWIPT for PLS in IoT considering these features. Firstly, V-MIMO come up with larger antenna gain (spatial multiplexing) to cope up the higher data rate and capacity for 5G applications [11]. Secondly, as multiple signals are transmitted from large number of antennas and these signals are combined in free space, the noise and fading have no effect at all resulting in robust and reliable systems. Thirdly, beamforming with large number of antennas, it avoids the fading dip in multipath with reduced latency at receiver side [12]. Forth, V-MIMO provide large degree of freedom at terminals so that it strengthens the secrecy rate against the interference or jamming signals due to unintended users. Fifth, jamming signals provides long lasting security to transmitted signal regardless of computing power of eavesdropper. It also reduces the cost of maintaining secret key distribution or management for scalable next generation 5G centric sensor enabled IoT [13].

In this context, this paper presents a novel secure V-MIMO SWIPT framework using beamforming and cooperative jamming signals to enhance the secrecy rate for 5G centric sensors-enabled IoT. Moreover, the secrecy rate maximization problem is solved by using the iterative algorithm which inherently applies the penalty function. The major contributions of the paper are as follows:

1) Firstly, a system model for V-MIMO SWIPT enabled IoT is presented focusing on its functionality and channel condition assumptions.
2) Secondly, a secure V-MIMO SWIPT framework is proposed considering beamforming and cooperative jamming schemes to compute the secrecy rate, total harvested energy and energy efficiency of the system.
3) Thirdly, the secrecy rate maximization problem is mathematically derived using beamforming vector, PS and TS ratio as optimization parameters.
4) Fourthly, the maximization problem is transformed into three convex sub-problems for jointly solving the problems using the penalty function and iterative algorithm.
5) Finally, simulations are performed to analyze the performance of the proposed technique in optimizing the secrecy rate of the V-MIMO SWIPT enabled IoT system.

The remaining paper is organized as follows. In section II, related works are critically reviewed. In section III, a secure V-MIMO SWIPT technique for 5G centric sensors-enabled IoT system is presented. In section IV, a maximization problem is formulated with solution. In section V, simulation results are discussed. In section VI, conclusion is presented.

II. Related Work

Numerous researches have been done in the area of providing energy efficient and secure communication in the wireless communication [14-25]. So far very few works have been done to combine the use of V-MIMO, SWIPT, beamforming and cooperative jamming in single system. In the interest of emphasizing the novelty of this paper, it is necessary to compare our work with the existing works.

Firstly, although multiple-input-single-output (MISO) scheme with cooperative jamming is investigated to increase the secrecy rate of the system [14-15], somewhere SWIPT technique for energy harvesting in V-MIMO transmission is missing out. In the paper [14], authors have used MISO information passing technique in addition with jamming signal to increase the SINR at the data gathering center and produce interference on the intruder channel respectively. Whereas in [15], for data rate maximization, the authorized transmitting node chooses an alternative route using relay to forward the data towards the sink instead of the direct route. However, neither SWIPT nor V-MIMO transmission is discussed to harvest energy and increase spectral efficiency and reliability of the network respectively. As, SWIPT and V-MIMO transmission plays an important role in improving the SINR at receiver side and reliability respectively in low-powered 5G centric sensors-enabled IoT network.

Secondly, although secure SWIPT-NOMA communication channel of primary user in cognitive radio network (CRN) has been investigated in [16-18], most of them only use beamforming MISO data transmission scheme, and whether it is suitable for V-MIMO transmission in IoT network or not is remain unanswered. In [16], authors have exploited the beamforming, SWIPT-NOMA and cooperative jamming technique in order to harvest energy and provide secure communication between main user and subordinate user nodes. In the papers [17, 18], secrecy beamforming scheme has been proposed which exploits the jamming signal technique into null range of main channel to protect the confidential information in the existence of eavesdropper. However, in [17] SWIPT technique has not been used to provide extra energy scavenging by receivers to send jamming signals and also has not studied the effect when the users are more than two. Whereas in [18], authors have proposed a joint optimal scheme using secure beamforming for underlay and alternating algorithm for cooperative schemes to minimize the total power consumption in CRN MISO transmission network. However, above literature has not mentioned any security scheme to protect the information in untrusted secondary user pairs and failed to describe the effect of multipath loss and fading in dynamic channel environment.

Thirdly, in order to increase the system secrecy rate in the presence of untrusted amplify and forward (AF) relay, PS or TS mode and destination based artificial noise addition to impair the channel of untrusted relay are investigated [19-22], under the assumption of perfect channel state information (CSI) for only MISO transmission, and energy efficiency of the system is not optimized. In [19], authors have proposed PS mode based local optimal and global optimal algorithms to boost the network secrecy rate by using beamforming and PS ratio as optimization variable. Whereas in [20], TS mode based for multiple sensors and multiple half-duplex untrusted AF relay, a novel best-sensor-best-untrusted-relay scheme has been proposed to improve the system secrecy rate. However, the performance of the scheme downgrades in the case of higher eavesdropping rate because the proposed scheme has not used jamming signal and beamforming to provide PLS. In [21], helper nodes are able to both harvest energy (SWIPT-MISO) and releasing the jamming signal, whereas in [22] helpers nodes only send the jamming signals to untrusted relay

communication channel and there is not used any EH scheme to compensate the energy consumption in transmitting jamming signal, which can cause the node failure problem. And, also external jammer nodes added up additional cost to the system, as well as computation time increases with respect to protocol [11], where full duplex relay is used without any external helper nodes.

Fourthly, combined key distribution design for both AL and PLS are discussed by authors in [23-25] limited to small key distribution and also did not mention any EH technique. Authors have proposed PLS based [23] and threshold cryptography based [24] key generation scheme as compare to the conventional key generation method. It reduces the number of key generations for deployment of secure network, whereas in [25] encryption-based schemes are investigated in near field wireless communication by using magnetic coupling to secure the network. Also, these schemes consume much more energy and computational power in encryption and key distribution respectively, thus these schemes are not suitable for energy-constrained 5G centric sensors-enabled IoT network.

III. Lightweight Security for V-Mimo Swipt System

A. System Model

We consider the energy efficient and secure information transmission in a wireless powered V-MIMO system as shown in the Fig. 1. The V-MIMO is a cluster-based network topology, where cluster head (CH) sends or receives data through cooperative nodes (CN). Further, a sink node collects data from the CH. Each node follows non-linear EH model under SWIPT for practical implementation to avoid performance loss. Where output DC power increases up to saturation limit with increase in input power. This is because non-linear model RF to DC conversion efficiency alters the output power according to input RF power level rather than remain constant as in linear EH model. Therefore, each CN uses non-linear EH SWIPT technique with combination of PS and TS protocols. It is clarified that in SWIPT, the power source of every sensor nodes for EH is radio signal itself. It means, while communicating with neighboring nodes, all the radio signal receiver nodes harvest energy. For realizing clusters without eavesdroppers, simply start with a single node and gradually includes neighboring sensor nodes with successful verification.

Each sensor is granted an omnidirectional antenna and equal initial power to function in half-duplex mode. Let us assume that 'A' and 'B' be the cluster heads of two separate neighbor clusters. The system consists of same number of CN (N) for both 'A' (transmitting cluster) and 'B' (receiving cluster) from the total number of nodes N_t and N_r. Let $C_A = \{C_i | i = 1, 2, 3 \dots, N\}$ and $C_B = \{C_j | j = 1, 2, 3 \dots, N\}$ represent the CN sets of 'A' and 'B' respectively. The number of CN are selected to minimize the overall energy consumption in data transmission for intra-cluster and inter-cluster communication. The channel is supposed to be an additive white Gaussian noise (AWGN) for intra-cluster free-space communication with squared distance($\boldsymbol{d_{ij}^2}$). Also, we assume that every CN undergoes frequency non-selective and slow Rayleigh fading (multipath communication) while inter-cluster data transmission takes place with biquadrates distance ($\boldsymbol{d_{ij}^4}$). Furthermore, independent fading coefficient is experienced by CN due to large distance between nodes with respect to wavelength. The reason behind assumption of such channel is that the distances between nodes within the cluster are much lesser than the inter-cluster distances.

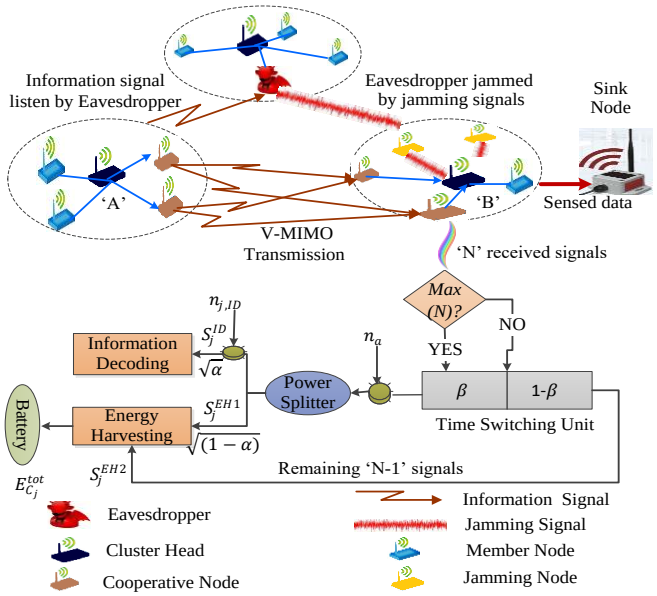

Fig.1. Communication Model for Secure V-MIMO SWIPT

B. Security Vulnerabilities Measures and Attack Model

Let us assume that eavesdropper 'e' is supposed to be a normal sensor node in another cluster. As, member nodes of same cluster already know about the information, therefore nodes in another cluster that are not aware of other clusters information are treated as eavesdropper. At the beginning of each time slot, transmitter sends the pilot signal to destination and channel state information (CSI) is evaluated by the receiver and feedback the CSI to transmitter similar to [26]. Eavesdropper is assumed to work in non-colluding mode i.e. it wiretap the main channel (eavesdropping the feedback message) independently and know the instantaneous CSI of main channel, but eavesdropper has no information about channel between receiver and itself. This is because receiver does not send any pilot signal to eavesdropper. So, the eavesdropper uses the instantaneous CSI of main channel for eavesdropping of secured transmitted message. To avoid eavesdropping, legitimate receiver-based jamming signal is released to distort the signal received by the eavesdropper.

The location of eavesdropper matters much for eavesdropping, as the secured message transmitted in the beamformed direction towards legitimate receiver. Overall, the system vulnerability depends upon channel condition and eavesdropper's location. In the simulation section-V-IV, we have performed the vulnerability test in detail. Further, if the eavesdropper also possess jamming nodes and try to neutralize the received interference by jamming signal of legitimate receiver, however it is not possible for eavesdropper to do so completely. Because the jamming signal transmitted by jamming nodes of legitimate receiver is of different power that is independent to each other and also coded with structured

codes (such as Gaussian noise distribution) which is orthogonally aligned to secured transmitted message [27]. Thus, it is very hard for eavesdropper to decode the jamming signals completely for nullify the effect of interference even in the case of presence of its own jamming nodes due to its limited capabilities of eavesdropping such as channel estimation errors (as it has no knowledge about channel between receiver and itself), different frequency of subtle RF components and error in the alignment of eavesdropper in the direction of secured beamformed transmitted signal. Whereas, only legitimate receiver knows about the jamming signal distribution code and also V-MIMO provides large null spaces to receiver where interference cancel out and nearly everything can be absorbed without affecting the receiver node. Thus, secrecy rate performance is enhanced by the cooperative orthogonal jamming technique without affecting the intended receiver.

C. Secure V-MIMO SWIPT Technique

Our focus is on a particular manifestation of a data transmission from A's cluster to B's cluster (see Fig. 1).

Case-1- When the eavesdropper '***e***' does not have any cooperative (jamming) nodes, and it tries to eavesdrop the secured transmitted signal only by intercepting the main channel without any jamming attack. The proposed technique operates in five steps as follow:

i) In the first step, the sensors collect the information from the monitoring region and transfer it to its CH ('A').

ii) After that, CH('A') aggregate the collected information.

iii) The CH ('A') broadcasts similar pre-processed information to its cooperative nodes using V-MIMO scheme. At the same time, in the above steps *i* and *iii*, some member nodes of B's cluster selected as jamming node that are represented as $J = \{J_k | k = 1, 2, 3 \dots, m\}$. These jamming nodes send jamming signals to 'B' in such a way that it belongs to the null space of B's channel. It is difficult for the eavesdropper to listen the confidential information during the intra-cluster communication in step *i* and *iii*. Because the inter-cluster distance for data transmission is significantly larger than the intra-cluster distance. Even if it is possible for eavesdropper to hear the transmitted signals in A's cluster, the received signal of eavesdropper is corrupted because of jamming signals. So, the information has been secured.

iv) The set of N cooperative nodes (C_A) in A's cluster acts a virtual antenna array for the implementation of linear beamforming method to transmit signal. The signal received by the CN C_i from 'A' in step *iii* is given as

$$S_i = b_i x + n_i \quad (1)$$

where b_i represents the $N - dimensional$ complex beamforming vector at the transmitting side cooperative node i i.e.; $b_i = [b_1, b_2, b_3, \dots, b_N]^T \in \mathbb{C}^{N \times 1}$ with $\mathbb{E}\left\{||b_i||^2\right\} = 1$, x denotes the information signal with power P, $\mathbb{E}\{|x|^2\} = P$, and n_i represents the circularly AWGN at the cooperative node $C_i$with zero mean and σ^2 variance, $n_i \sim CN(0, \sigma^2)$. The jamming signal (independent and identically distributed Gaussian noise) sent by J_k is represented by $a_k = diag\big((\sqrt{P_1}, \sqrt{P_k} \dots \dots \sqrt{P_m})(J_1, J_k \dots J_m)\big)$, where P_k is power of k^{th} jamming node and satisfy $P_J = \sum_{k=1}^{m} P_k$ for $k = 1, 2, 3, \dots, m$. Thus, the signal received S_{B1} at 'B' is given as sum of the jamming signal received in *i* and *iii* steps.

$$S_{B1} = 2\sum_{k=1}^{m} a_k + n_{B1}\text{, where } n_{B1} \sim CN(0, \sigma^2) \quad (2)$$

v) Further, the CN of 'A' encode and transmit the encoded message to CN of 'B' with the help of V-MIMO scheme using orthogonal space-time block codes (STBC) and finally towards the sink node.

vi) The receiving node receives multiple copies of the same transmitted signal. To extract as much useful information, it combines the entire received signal and process it linearly to reduce the system complexity according to the improved version of STBC referred to [28] and finally decoded information is transferred to 'B'. In the meantime, the same jamming signal is transmitted to 'B' by the jamming nodes of B's cluster in step *iv* and *v*. 'B' can neutralize the effect of jamming signals by subtracting the signals received at step *i* and *iii* from signal received at step *iv* and *v*, as it has knowledge about the jamming signals. Hence, it is not affected by the jamming signals.

Here we assume uniform PS and TS ratio for all receiving nodes (C_j). Let T indicates the extent of each data transmission period. Each data transmission period is divided into two time slots i.e., βT and $(1-\beta)T$, where $0 < \beta \leq 1$. Cooperative node at 'B' receives N replicas of same transmitted signal from A's cooperative nodes. In βT time duration, the B's cooperative node C_j apply PS scheme for simultaneous EH and ID. In this scheme, the strongest signal is selected from 'N' received signals and is sent to the power splitter. Power splitter splits the power of the selected signal into ratio α and $(1-\alpha)$ for simultaneous ID and EH respectively, where $0 < \alpha \leq 1$. For $(1-\beta)T$ time duration, there is no PS and the whole remaining $(N-1)$ received signals are passed through EH circuit (see Fig. 2). Thus, the CN are able to harvest more energy to support V-MIMO communication which in turn increases energy efficiency of the system.

Let H_{ij} represents the V-MIMO channel gain matrix between C_i and C_j, h_{ie} indicates the channel gain between $C_i$and eavesdropper, q_{ke} indicates the channel gain between J_k and eavesdropper. After applying the SWIPT technique, the signal for information decoding at B's cooperative node C_j in βT time duration is modelled as

$$S_j^{ID} = \sqrt{\alpha}(H_{ij} b_i x + H_{ij} n_i) + n_{j,ID},$$
$$\forall C_j \in C_B, j = 1, 2, 3, \dots, N; C_i \in C_A, i = 1, 2, 3, \dots, N \quad (3)$$

where $n_{j,ID} \sim CN(0, \partial^2)$ is the circularly AWGN for ID produced by radio frequency to baseband conversion at C_j. The signal for EH at C_j in βT time duration is given as

$$S_j^{EH1} = \sqrt{(1-\alpha)}(H_{ij} b_i x + H_{ij} n_i),$$
$$\forall C_j \in C_B, j = 1, 2, 3, \dots, N; C_i \in C_A, i = 1, 2, 3, \dots, N \quad (4)$$

Now, for $(1-\beta)T$ time duration, the signal for energy harvesting at C_j is given as

$$S_j^{EH2} = \sum_{i=1}^{N-1} H_{ij} b_i \, x + \sum_{i=1}^{N-1} H_{ij} n_i,$$

$$\forall C_j \in C_B, j = 1,2,3,\dots,N; C_i \in C_A, i = 1,2,3,\dots,N \quad (5)$$

Therefore, the total energy harvested at C_j for time period T is given as

$$E_{C_j}^{tot} = \varepsilon_j \eta_j \left\{ \left(\beta T (1-\alpha) \left(P \left| H_{ij} b_i \right|^2 + \left| H_{ij} \right|^2 \sigma^2 \right) \right) + \left(((1-\beta)T) \left(\sum_{i=1}^{N-1} P \left| H_{ij} b_i \right|^2 + \sum_{i=1}^{N-1} \left| H_{ij} \right|^2 \sigma^2 \right) \right) \right\}, \quad \forall C_j \in C_B \quad (6)$$

where $0 < \varepsilon_j < 1$ is the EH coefficient for C_j, $0 < \eta_j < 1$ represents energy conversion efficiency for C_j in transforming the received RF signal to DC so that it can be stored for later use, which relies on the EH circuit and the rectification process. And the average EH for the given duration T is

$$E_{C_j}^{Avg} = \varepsilon_j \eta_j \{ \left(\beta (1-\alpha) \left(P \left| H_{ij} b_i \right|^2 + \left| H_{ij} \right|^2 \sigma^2 \right) \right) + \left(((1-\beta)) \left(\sum_{i=1}^{N-1} P \left| H_{ij} b_i \right|^2 + \sum_{i=1}^{N-1} \left| H_{ij} \right|^2 \sigma^2 \right) \right) \}, \quad \forall C_j \in C_B \quad (7)$$

Now, the signals received at 'B' and eavesdropper after step *v* can be respectively given as

$$S_{B2} = \left(\sum_{j=1}^{N} \sqrt{\alpha} (H_{ij} b_i \, x + H_{ij} n_i) + n_{j,ID} \right) + 2 \sum_{k=1}^{m} a_k + n_{B2} \quad (8)$$

$$S_e = \sum_{i=1}^{N} (h_{ie} b_i \, x + h_{ie} n_i) + \sum_{k=1}^{m} q_{ke} a_k + n_e \quad (9)$$

where $n_{B2} \sim CN(0, \sigma^2)$, $n_e \sim CN(0, \sigma^2)$. After subtracting S_{B2}-S_{B1}, the signal at 'B' is given as

$$S_B = \left(\sum_{j=1}^{N} \sqrt{\alpha} (H_{ij} b_i \, x + H_{ij} n_i) + n_{j,ID} \right) + n_B \quad (10)$$

where $n_B \sim CN(0, \sigma^2)$

Accordingly, the SINR at 'B' and eavesdropper can be respectively given as

$$\gamma^B = \frac{\sum_{j=1}^{N} \alpha P |H_{ij} b_i|^2}{\sum_{j=1}^{N} \alpha |H_{ij}|^2 \sigma^2 + \partial^2 + \sigma^2} \quad (11)$$

$$\gamma^{Ed} = \frac{\sum_{j=1}^{N} P |h_{ie} b_i|^2}{\sum_{j=1}^{N} |h_{ie}|^2 \sigma^2 + \sum_{k=1}^{m} |q_{ke} a_k|^2 + \sigma^2} \quad (12a)$$

$$\leq \frac{\sum_{j=1}^{N} P |h_{ie} b_i|^2}{\sum_{k=1}^{m} |q_{ke} a_k|^2 + \sigma^2} \quad (12b)$$

Where (12a) shows that the worst-case possibility of decoding the secured transmitting message at eavesdropper constitutes upper bound on SINR and for eavesdropper not able to decode secured message, γ^{Ed} must satisfy the inequality of Eq. (12b).

Case-2- When eavesdropper '*e*' has its own jamming nodes, it tries to neutralize the effect of interference produced by the jamming nodes of legitimate receiver and, to enhance its probability of eavesdropping simultaneously. It is a kind of jamming attack by eavesdropper. In this case, the transmission of data and energy harvesting procedure follow the same steps as in case-1 up to Eq. (8). The signal received by eavesdropper '*e*' after step *v* as follow;

$$S_e = \sum_{i=1}^{N} (h_{ie} b_i \, x + h_{ie} n_i) + \Phi \sum_{k=1}^{m} q_{ke} a_k + n_e \quad (13)$$

where Φ is the residual jamming interference ratio ($0 \leq \Phi \leq 1$). When $\Phi = 0$, eavesdropper is assumed to be ideal and able to cancel out all the interference caused by receiver. Thus, secured message is listened by eavesdropper, it shows system failure. When $\Phi = 1$, it shows that jamming signal produced by eavesdropper is very weak and not able to mitigate the effect of interference at all, treated as Case-1, which reduced to Eq. (9). In practical standpoint view the value of $\Phi \in (0,1)$.

The eavesdropper can only partially mitigate the interference received from CN of 'B'. Accordingly, the SINR at 'e' is given as follow

$$\gamma^{Ed} = \frac{\sum_{j=1}^{N} P |h_{ie} b_i|^2}{\sum_{j=1}^{N} |h_{ie}|^2 \sigma^2 + \Phi \sum_{k=1}^{m} |q_{ke} a_k|^2 + \sigma^2} \quad (14a)$$

$$\leq \frac{\sum_{j=1}^{N} P |h_{ie} b_i|^2}{\Phi \sum_{k=1}^{m} |q_{ke} a_k|^2 + \sigma^2} \quad (14b)$$

Note that if $\Phi = 1$, jamming nodes of the eavesdropper are worthless and it has no impact on the cancellation of interference. Where (14a) shows that the worst-case possibility of decoding the secured transmitting message at eavesdropper constitutes upper bound on SINR, and for eavesdropper to not be able to decode secured message, γ^{Ed} must satisfy the inequality of Eq. (14b).

D. Secrecy performance analysis

(i) Achievable Secrecy rate

In accordance to Shannon's formula the obtained average data rate from 'A' to 'B' and 'A' to eavesdropper can be respectively given as

$$R^{AB} = \beta W \log_2(1 + \gamma^B) \quad (15)$$

$$R^{AE} = \beta W \log_2(1 + \gamma^{Ed}) \quad (16)$$

where, W denotes the channel bandwidth. For a successful transmission, the received γ^B must be greater than threshold value γ^{min} and received γ^{Ed} must be less than γ^{min}. Accordingly, R^{sec} must be greater than threshold value R^{min}. The subtraction between the data rate of main channel and the intercepted channel is defined as the achievable secrecy rate at the 'B'.

$$R^{sec} = \begin{cases} (R^{AB} - R^{AE})^+ & if \ \gamma^B > \gamma^{Ed} \\ 0 & if \ \gamma^B < \gamma^{Ed} \end{cases} \quad (17)$$

Where, $(z)^+ = \max(z, 0)$. If $\gamma^B < \gamma^{Ed}$, then eavesdropper cancel out interference produced by receiver in case of lower SINR of main channel and enforce the transmitter for retransmission of secured message, which increases the probability of eavesdropping.

(ii) Success Probability

It is introduced to measure the success probability of legitimate receiver $P(A,B)$ or eavesdropper $P(A,ED)$ with regard to decode the secured transmitted message. For successful and secure transmission, the success probability $P(A,B) = P(\gamma^B \geq \gamma^{min})$ and unsuccessful probability $P'(A,ED) = P(\gamma^{Ed} \leq \gamma^{min})$ both threshold should be met. Where, $P'(A,ED) = 1 - P(A,ED)$. For example, if the γ^{Ed} is higher than the predefined γ^{min} of secure message designed, the secured message transmission failed even in the case of γ^B higher than γ^{min}. And, there may be case of retransmission, if the γ^B is less than γ^{min} and much serious case of failure in addition to above case if the value of γ^{Ed} is greater than γ^{min}. Thus, the achievable secrecy rate R^{sec} depends upon ordered pair of success probability $(P(A,B), P(A,ED))$.

The $P(A,B)$ defines the probability that the main channel is not in outage, *i.e.*, there is successful transmission between transmitter and receiver given as

$$P(A,B) = P(\gamma^{\boldsymbol{B}} \geq \gamma^{min}) = e^{-n_B \gamma^{min} \sum_{j=1}^{N} \alpha P |H_{ij} b_i|^2} \quad (18)$$

The $P(A,ED)$ define the probability that eavesdropper successfully decode the secured message can be given as

$$P(A,ED) = P(\gamma^{Ed} \geq \gamma^{min})$$
$$= e^{-n_e \gamma^{min} \sum_{j=1}^{N} P|h_{ie} b_i|^2} \mathbb{E}_{\boldsymbol{h_{ie}}} \left[e^{-\gamma^{min} \sum_{j=1}^{N} P|h_{ie} b_i|^2 \sum_{j=1}^{N} |h_{ie}|^2 \sigma^2 \Phi \sum_{k=1}^{m} |q_{ke} a_k|^2} \right]$$
$$= e^{-n_e \gamma^{min} \sum_{j=1}^{N} P|h_{ie} b_i|^2} (\prod_{j=1}^{N} \frac{1}{1+\gamma^{min} \sum_{j=1}^{N} P|h_{ie} b_i|^2 \sum_{j=1}^{N} |h_{ie}|^2 \sigma^2 \Phi \sum_{k=1}^{m} |q_{ke} a_k|^2}) \quad (19)$$

E. Energy Consumption

We can easily notice that the energy efficiency of a V-MIMO system can be enhanced by harvesting energy, since the system power consumption is neutralized with the harvested power. The power consumption in intra cluster communication is smaller than inter cluster transmission [36]. The total power consumption (P_c) in intra-cluster communication divided into two parts (i) power consumption (P_{HN}) in CH to cooperative nodes (ii) power consumption (P_{NH}) in cooperative nodes to CH.

$$P_c = P_{HN} + P_{NH} \quad (20)$$

$$P_{HN} = (1+\mu) n_i \sigma^2 \ln(p_b) G_{d1} d_{max}^2 L_m + \frac{p_{tc} + N p_{rc}}{w} \quad (21)$$

$$P_{NH} = (1+\mu) n_i \sigma^2 \ln(p_b) G_{d1} d_{max}^2 L_m + \frac{N p_{tc} + p_{rc}}{w} \quad (22)$$

where μ (≥ 1)denote the inefficacy of the transmitter's power amplifier, p_b denote the bit error rate performance of binary phase shifting key. The gain factor at free-space distance $d_{max}^2 = 1m$ is denoted by $G_{d1}$and L_m denotes the link margin. The power consumption in transmitting circuit (p_{tc}) and receiver circuit (p_{rc}) is fixed.

In the inter-cluster communication, the total power consumption (P_f) in N cooperatives nodes of transmitting cluster calculated as follow

$$P_f = (1+\mu) \frac{N_o}{{p_b}^{1/i}} \sum_{i=1}^{N} \frac{(4\pi)^2 d_{ij}^4}{G_t G_r \lambda^2} L_m n_j + \frac{N(p_{tc} + p_{rc})}{w} \quad (23)$$

where N_o denote spectral density of single side as noise power, the multipath distance between cooperative node is represented by d_{ij}^4; G_t and G_r denotes the antenna gain of transmitter and receiver,$n_j$denotes the noise at receiver side.

And, The Power consumption in jamming signals from jammer node of receiving node is $P_J = \sum_{k=1}^{m} P_k$ for $k = 1, 2, 3, \dots, m$. In particular, the total power consumption in transmitting the data from 'A' to 'B', E_{TC} under time slot T as follow;

$$E_{TC} = P_c T + P_f T + P_J T - \sum_{j=1}^{N} E_{C_j}^{tot} \quad (24)$$

$$\forall C_i \in C_A, i = 1, 2, 3, \dots, N; \forall C_j \in C_B, j = 1, 2, 3, \dots, N$$

where, $\sum_{j=1}^{N} E_{C_j}^{tot}$ represents the total energy harvested, which is interpreted as remuneration energy of the network system.

The sum total data bits propitiously sent to the B's cluster per Joule utilized energy is interpreted as the average energy efficiency for 'B' and is given as

$$\psi = \frac{R^{AB}}{E_{TC}} \quad (25)$$

IV. The Maximization Problem and Its Solution

A non-linear maximization problem is mathematically formulated to collectively optimize the beamforming vector, PS ratio and TS ratio for system secrecy rate maximization R^{sec} given in Eq. (17). The rationale behind taking beamforming vector b_i is that, it is responsible for enhancing the achievable secrecy rate by transmitting the confidential message in the direction of intended receiver rather than omni-directional transmission. That put extra effort for eavesdropper to align in the same direction or location between the communicating nodes in order to eavesdrop the secured message. Whereas, PS ratio and TS ratio is responsible for energy harvesting and information decoding (SINR) at receiver side. The lower value of information decoding PS splitting ratio α leads to less decoding of secured message but harvest more energy, similar for higher value of information TS ratio β leads to more successfully decode the received secured message but lower down the harvested energy by nodes. Overall, unbalanced splitting ratio of PS and TS unit leads to decrease in achievable secrecy rate. So, there is trade-off between energy harvesting time, information decoding time and secure transmitted beamforming signal vector for enhancing the achievable secrecy rate (for discussion see Section-VI). Thus, the mathematical problem can be given as

$$\text{(P1):} \quad \max_{b_i, \alpha, \beta} R^{sec}(b_i, \alpha, \beta) \quad (26)$$

Subject to- C_1: $||b_i||^2 \leq 1, \forall C_i \in C_A, i = 1, 2, 3, \dots, N$

C_2: $E_{C_j}^{Avg} \geq E_{min}, \forall C_j \in C_B, j = 1, 2, 3, \dots, N$

C_3: $0 < \alpha \leq 1$

C_4: $0 < \beta \leq 1$

where C_1 indicates the constraint on beamforming vector, C_2 indicates that the energy harvested from the received signals must be greater than the minimal energy harvesting need of cooperative nodes. The C_3 and C_4 denote the PS ratio and TS ratio constraints respectively. The formulated problem is non-convex because of the coupling among the optimization variables $b_i, \alpha,$ and β under the constraint $C1$ to $C4$. As, $E_{C_j}^{Avg}$ depends upon both α and β. And also, the complexity of maximization of achievable secrecy rate is high in regard of finding solution because of concave function for b_i when the values for α and β are kept as a constant and *vice versa*. Thus, it is not feasible to solve the problem simultaneously with the three optimization variables(b_i, α, β). Therefore, to reach the feasible solution of the given problem P1; we present an iterative algorithm-1 in the following section. The convergence property of the algorithm can be mathematically proven. To solve the non-convex maximization problem P1, in the next sub-section the original maximization problem splits into three convex sub-problems [29].

A. *Optimal Beamforming*

For the constant value of PS ratio α and TS ratioβ, the optimal value of the beamforming vector $b_i$for each cooperative node $C_i$can be obtained by maximizing the secrecy rate.

$$\text{(P 2.1):} \max_{b_i} R^{sec}(b_i) \quad (27)$$

$$\text{s.t.} ||b_i||^2 \leq 1, \forall C_i \in C_A, i = 1, 2, 3, \dots, N$$

$$E_{C_j}^{Avg} \geq E_{min}, \forall C_j \in C_B, j = 1, 2, 3, \ldots, N$$

Now, we solve the above problem using penalty function method with penalty parameter γ for the optimal solution. The optimum solution to the problem (23) is computed as

$$b_i{}^* = \frac{\sqrt{2}\sqrt{(S_1(S_1 - S_2))}}{2S_1} \quad (28)$$

Where $S_1 = (\varepsilon_j \eta_j \beta(1-\alpha) P H_{ij}^2) + (\varepsilon_j \eta_j (1-\beta)(\mathrm{N}-1) P H_{ij}^2)$

$S_2 = (\varepsilon_j \eta_j \beta(1-\alpha) H_{ij}^2 \sigma^2) + (\varepsilon_j \eta_j (1-\beta)(\mathrm{N}-1) H_{ij}^2 \sigma^2 + E_{min}$

B. Optimal Power Splitting Ratio

For the above achieved value of b_i and the given constant value β, the optimal value of α can be obtained by maximizing the secrecy rate. The secrecy rate $R^{sec}(\alpha)$ is concave on PS ratio α and it can be expressed as:

$$\text{(P 2.2)}: \max_{\alpha} R^{sec}(\alpha) \quad (29)$$
$$\text{s.t. } 0 < \alpha \leq 1$$
$$E_{C_j}^{Avg} \geq E_{min}, \forall C_j \in C_B, j = 1, 2, 3, \ldots, N$$

Now, we solve the above problem using penalty function method with penalty parameter γ for the optimal solution. The optimum solution to problem (25) is computed as

$$\alpha^* = 1 - \frac{(E_{min} - F_1)}{(2 * F_2)} \quad (30)$$

where $F_1 = \varepsilon_j \eta_j (1-\beta)(\mathrm{N}-1)(P H_{ij}^2 b_i{}^2 + H_{ij}^2 \sigma^2$

$F_2 = \varepsilon_j \eta_j \beta (P H_{ij}^2 b_i{}^2 + H_{ij}^2 \sigma^2)$

C. Optimal Time Switching Ratio

For the above achieved value of b_i and α, the optimal value of time switching ratio β can be achieved by maximizing the secrecy rate.

$$\text{(P 2.3)} \quad \max_{\beta} R^{sec}(\beta) \quad (31)$$
$$\text{s.t. } 0 < \beta \leq 1$$
$$E_{C_j}^{Avg} \geq E_{min}, \forall C_j \in C_B, j = 1, 2, 3, \ldots, N$$

Now, we solve the above problem using penalty function method with penalty parameter γ for the optimal solution. The optimum solution to problem (27) is computed as

$$\beta^* = \frac{G_1(G_2 - G_3) - \sqrt{4\gamma^2 G_2{}^2 + G_1{}^2 G_2{}^2 + 2 G_1{}^2 G_2 G_3 + G_1{}^2 G_3{}^2 + 2\gamma G_2}}{2 G_1 G_2} \quad (32)$$

where $G_1 = W \log_2\left(\frac{H_{ij}^2 \sigma^2 + m |q_{ke} a_k|^2 + \sigma^2}{H_{ij}^2 \sigma^2}\right)$

$G_2 = (P H_{ij}^2 b_i{}^2 + H_{ij}^2 \sigma^2)((\varepsilon_j \eta_j (1-\alpha)) - (\varepsilon_j \eta_j (N-1)))$

$G_3 = (\varepsilon_j \eta_j (N-1)\ (P H_{ij}^2 b_i{}^2 + H_{ij}^2 \sigma^2)) - E_{min}$

It is clarified that the initial value of the TS ratio ($\beta = 0.01$) and PS ratio ($\alpha = 0.01$) is set according to heuristic approach. The optimal value of TS ratio ($\beta = 0.56$) and PS ratio ($\alpha = 0.42$) obtained for transmitted power 20 dBm in our experimental validation.

D. Iterative Algorithm for Secrecy Rate Maximization

We now present an iterative algorithm-1 to give the solution of the maximization problem P1 in (22). To initialize the algorithm, proper value of the variables b_i, α, and β are set according to heuristic approach for iteration number $n = 0$ as $b_i{}^0, \alpha^0 and\ \beta^0$. The presented iterative algorithm runs for either maximum number of iteration or till the secrecy rate converges. Finally, the optimal value of the variables at which secrecy rate maximized is obtained. The presented iterative algorithm gives guarantee to converge the secrecy rate at maximum value with a smaller number of iterations regardless of choosing proper set of variables is the novelty of algorithm. And, also the heart of iterative algorithm is penalty function method, which convert constrained maximization problem into sequential unconstrained maximization problem by adding penalty terms to objective function for infeasibility [30].

The time complexity of Iterative algorithm-1 mainly depends upon penalty function method to obtain optimal value of $\{b_i{}^*, \alpha^*, \beta^*\}$ variables. The penalty function method iterate: say q times and add γ times penalty parameter to objective function towards optimality and feasibility. In steps (3-5) each time penalty function method is used to update the variables b_i, α, and β with complexity $O(q)$ and it runs for maximum number of iteration It_{max} as defined in outer loop (step-2). Thus, overall worst case time complexity of iterative algorithm-1 is $O(It_{max}(O(q) + O(q) + O(q))) = O(It_{max} q)$.

Algorithm-1: Iterative algorithm for secrecy rate maximization

Input:

It_{max}: Maximum number of iterations;

n: Iterative index;

Output:

$\{b_i{}^*, \alpha^*, \beta^*\}$: Optimal solution for beamformer, PS ratio and TS ratio.

Process:

1. Initialize $b_i{}^0, \alpha^0 and\ \beta^0$ with a proper value. Calculate $R^{sec}(b_i{}^0, \alpha^0, \beta^0)$ Set $n = 0$.
2. **while** n ≤ It_{max} **do**
3. For the constant value of α^n, β^n, find the solution $b_i{}^{n+1}$ using (24)
   // maximize (P 2.1): $\max_{b_i} R^{sec}(b_i)$ under penalty function method
4. By using $b_i{}^{n+1}$ and constant value of β^n, find solution of α^{n+1} using (26)
   // maximize (P 2.2): $\max_{\alpha} R^{sec}(\alpha)$ under penalty function method
5. By using the achieved value of $b_i{}^{n+1}$ and α^{n+1}, find the solution of β^{n+1} using (28).
   // maximize (P 2.3): $\max_{\beta} R^{sec}(\beta)$ under penalty function method
6. Calculate the secrecy rate $R_{n+1}^{sec} = R^{sec}(b_i{}^{n+1}, \alpha^{n+1}, \beta^{n+1})$.
7. **if** R_{n+1}^{sec} converges to optimal solution **then**
9. **return** $(b_i{}^*, \alpha^*, \beta^*) = (b_i{}^{n+1}, \alpha^{n+1}, \beta^{n+1})$
10. **else**
11. $n = n + 1$
12. **end if**
13. **end while**

Table 1. Simulation Parameters

Parameter	Value	Parameter	Value
P	$\{5, 10, 15, 20, 25, 30\}\ dBm$	α	(0.1,0.2 ….0.9, 1)
η	*0.7*	β	{0.1, 0.2,…,0.9,1}
W	$10^3\ Hz$	μ	*1*
L_m	40 *dB*	σ^2	10 *dBm*
P_{max}	30 *dBm*	E_{min}	0.01 *Joule*
H_{ij}	4	ε	0.8
p_{tc}	*22dBm*	p_{rc}	*20dBm*
G_{d1}	30*dB*	$G_t G_r$	5*dBi*
T	30 *sec*	∂^2	10*dBm*

V. Simulation and Results

In the given section, we present the simulation outcomes to illustrate the secrecy rate and energy efficiency of the proposed scheme under different performance metrics. In the simulation, we consider that 200 sensors are indiscriminately deployed over $100 \times 100\ m^2$ area. Similar initial power is provided to all the sensors in their rechargeable batteries, and

the corresponding parameters are provided in Table 1. Simulations are categorized into three sections to show the effectiveness of proposed scheme as- (I) performance analysis, (II) Comparative analysis, (III) Robustness analysis.

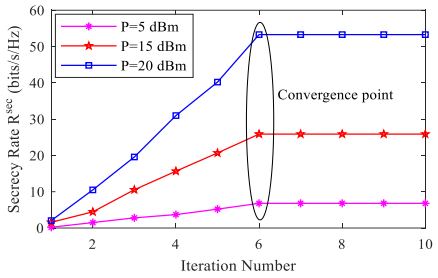

Fig. 2. Secrecy rate over iteration number with varying transmit power

A. *Convergence and Performance of the Iterative Algorithm*

Fig. 2 shows the convergence rate/effectiveness of the iterative algorithm-1 for distinct values of transmit power $P = \{5, 15, 20\}$ dBm of the CN. For initial setup the value of $\alpha = 0.01$, $\beta = 0.01$ *and* $b_i = 0.1$ are fed into algorithm-1 and these values are noted after each iteration until secrecy rate converges under different transmit power. As value of these parameters set in the penalty function either from experimental data or heuristic approach. Here we are using heuristic approach for setting-up initial values in penalty function method based iterative algorithm-1. The final value of parameters α, β and b_i for different value of P at which the secrecy rate converges are given as- at $P = 5$ dBm the value of $\alpha = 0.8$, $\beta = 0.3$ and $b_i = 0.09$; $P = 15$ dBm the value of $\alpha = 0.65$, $\beta = 0.39$ and $b_i = 0.05$; $P = 20$ dBm the value of $\alpha = 0.42$, β =0.56 and $b_i = 0.063$. After inspecting the outcomes of Fig. 2, it can be perceived that with the increment of P and iteration number, the secrecy rate of the system also improves, after that the algorithm converges within 6 iterations in every considered situation. The reason behind is as the P value of the CN intensifies; it enhances the signals' strength, and accordingly enhances the secrecy rate on increasing SINR at the authorized receiver.

B. *Impact of Transmit Power on Secrecy Rate*

Fig. 3(a)-(d) show the remarkable effect of transmit power P of the cooperative nodes on secrecy rate of the system with optimized PS ratio α^*, predetermined PS ratio $\alpha = [0.1, 1]$, After analyzing the results it can be observed that on intensifying the value of P of cooperatives nodes up to 20 dBm the secrecy rate of the system is a monotonically non-decreasing function of transmit power. i.e. the system performance is affected in constructive way. It is because, increasing value of P increases the signal's strength that assists the receiving CN to harvest additionally more energy, which enhances the SINR at the receiving cluster. Further, enhancing the value of P increases the strength of the source's node information signal. This leads to significant confidential information leakage towards the eavesdropper.

After that, with further increasing the P above 20 dBm, there is more information leakage through transmitting CN and it is listened by the eavesdropper, finally secrecy rate does not increase as much as previously increasing rate between 0 to 20 dBm for PS ratio in both cases i.e., α^* and α, which affects the network system in destructive way. Further, since fixed α is not the optimal solution, the secrecy rate or SINR is always less than the optimal value for all values of P. The reason behind is that for fixed α , harvested energy and decoded information is not enough for data transmission to its CH or next hop. As it can be observed from the Fig. 3(a)-(d) that, for $P = 20$ dBm and above the optimal value of PS ratio is about $\alpha^* = 0.42$, at which the secrecy rate is highest, and for other value of α the secrecy rate decreases. Furthermore, as the value of β increases it allows the receiver to spend more time in information decoding (improves SINR), so finally enhance secrecy rate of the system. Thus, it is clearly understood that optimal α^* can significantly improve the secrecy rate.

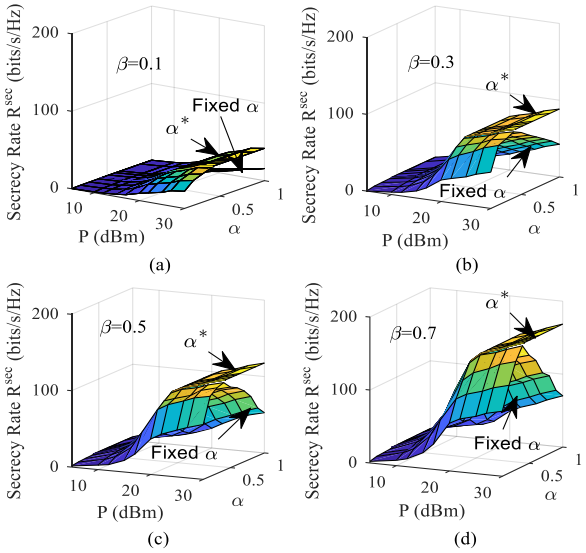

Fig. 3. Secrecy rate over transmit power and PS ratio α for (a) $\beta = 0.1$, (b) $\beta = 0.3$, (c) $\beta = 0.5$, (d) $\beta = 0.7$

C. *Secrecy Rate versus Energy Conversion Efficiency*

Fig. 4(a)-(d) show the simulation results carried out for analyzing the remarkable effect of energy conversion efficiency η of the CN on system secrecy rate for different values of α and β such as $\alpha = (0\ 1]$ and $\beta = \{0.2, 04, 0.6, 0.8\}$. Higher value of η permits CN to harvest additional amount of energy, so these CN in turn are able to enhance its transmit power. As a result, it enhances the system secrecy rate on improving SINR at the receiver. As, dictated by non-linear EH model, it limits the transmit power of the cooperative nodes on increasing value η , which is a favorable condition to keep secrecy rate higher. Otherwise signal with higher transmission power and energy conversion efficiency coefficient leads to information leakage and ultimately lower down the system secrecy rate. Consequently, in each case it has been found from simulation results that initially with the increasing value of η secrecy rate shoots up rapidly, but after $\eta = 0.5$ there is a slow increase in the secrecy rate for higher value of η. The results also illustrate that secrecy rate is more with low value of α, *and* β and worst increment with the higher value of α, *and* β. The reason behind is less value of α provide smaller proportion of the power received for processing information and larger proportion for harvesting

energy. Further for small value of β, system spend less time in PS mode for processing information and harvesting energy from received single signal with high intensity, and spend more time for harvesting energy from the remaining $N-1$ received signals, which further enhances the secrecy rate of the system.

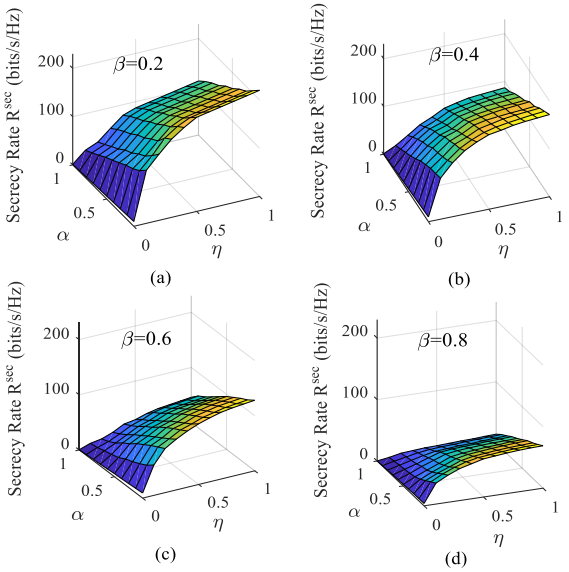

Fig.4. Secrecy rate over energy conversion efficiency and PS ratio α for (a) $\beta = 0.2$,(b) $\beta = 0.4$, (c) $\beta = 0.6$, (d) $\beta = 0.8$

D. Energy Efficiency versus Number of Cooperative Nodes

Fig. 5(a)-(d) show the simulation results carried out for analyzing the effect of cooperative nodes (N) on system average energy efficiency (ψ) for different values of α and β such as $\alpha = (0\ 1]$ and $\beta = \{0.2, 04, 0.6, 0.8\}$. It can be observed that, the average energy efficiency of the system initially improves with the increment of CN up to $N = 12$, after that decreases with the increment of N. The reason behind is that with increase in the number of cooperative nodes after a definite number, total energy consumption of the system also increases linearly. Further, energy consumption is taken into consideration for the formulation of energy efficiency using Eq. (21). Thus, large number of CN negatively affects the system energy efficiency. It can also be observed from the Fig. 6(a)-(d) that, with increase in the value of α and β the system energy efficiency decreases. Thus, the system is highly energy efficient for low value of $\alpha, and\ \beta$ and less energy efficient for high value of $\alpha, and\ \beta$. The reason behind is that for low value of α cooperative nodes use more fraction of received power for EH and for low value of β it spend more time in EH mode. Thus, nodes harvest more energy from the received signal and compensate the energy consumptions, which as a result enhance the system energy efficiency.

E. Comparison of Secrecy Rate over Cooperative Nodes

Fig. 6 manifests the secrecy rate performance with respect to number of transmit cooperative nodes (N) of the proposed V-MIMO SWIPT (EH+AN) scheme against without energy harvesting (w/oEH +AN) scheme mention in paper [12] using AN only, another scheme (w/oEH+BF) is using beamforming only without any EH scheme [14]. From the results it can be analyzed that, with increase in the cooperative nodes the system secrecy rate increases. Thus, the proposed V-MIMO SWIPT scheme with greater number of CN and EH circuit provides enhanced spatial degree of freedom and more energy respectively to maximize the system secrecy rate. It is clearly observed that the scheme without EH and only rely on beamforming as worst secrecy rate. Whereas, the scheme that uses both EH+AN techniques provide higher SINR at the authorized receiver, which as a result enhances the system secrecy rate with the increased cooperative nodes. The reason behind is that jamming signal create noise to eavesdroppers so that it cannot identify the information signal and also energy harvesting unit is able to harvest more energy, thus secrecy rate is maximized. Overall, V-MIMO SWIPT scheme achieves $19\%, 42\%, 75\%$ higher secrecy rate than w/oEH+AN scheme, EH+BF and w/oEH +BF scheme under number of cooperative nodes 20.

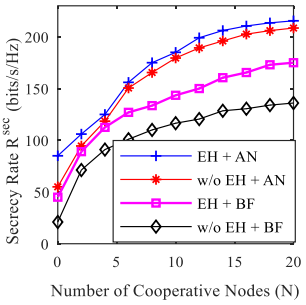

Fig.6. Secrecy rate over number of cooperative nodes

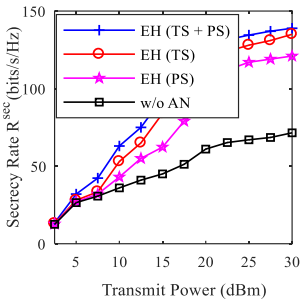

Fig.7. Comparison of secrecy rate against transmit power

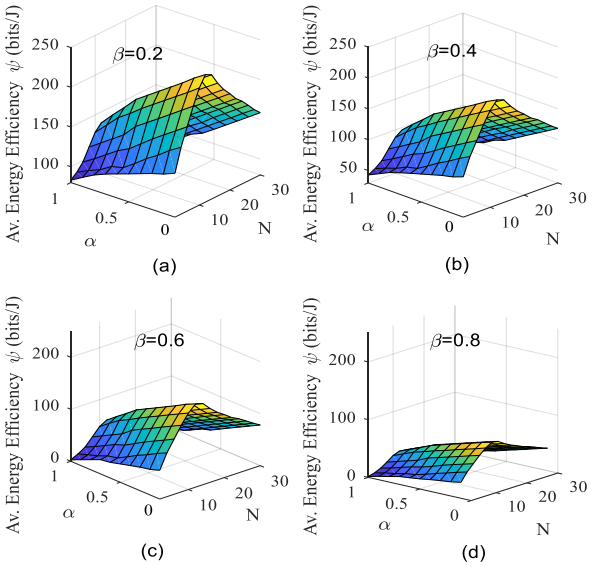

Fig.5. Average energy efficiency over number of cooperative nodes and PS ratio α for (a) $\beta = 0.2$, (b) $\beta = 0.4$, (c) $\beta = 0.6$, (d) $\beta = 0.8$

F. Comparison of Secrecy Rate versus Transmit Power

Fig. 7 illustrates the comparison of proposed V-MIMO SWIPT EH (TS+PS) enabled technique with V-MIMO enabled state-of-art techniques, only difference in their EH approach. It is evident from the result that the secrecy rate performance of the proposed technique is better (about 18%) than the scheme having feature of V-MIMO and TS mode of

SWIPT technique EH (TS) [11] (with BF and AN). This is because of more amount of EH from both, higher power single signal in PS mode and from remaining N-1 signal in TS mode. Whereas, the scheme with V-MIMO and only PS enabled SWIPT technique EH (PS) [19] (with BF and AN) has improved secrecy rate about 81% than the scheme with V-MIMO and without using artificial noise (w/o AN) (with BF and EH) but lower than EH (TS) scheme. Overall, proposed scheme has 18%, 32% and 90% improved secrecy rate than EH (TS), EH (PS) and w/o AN technique respectively.

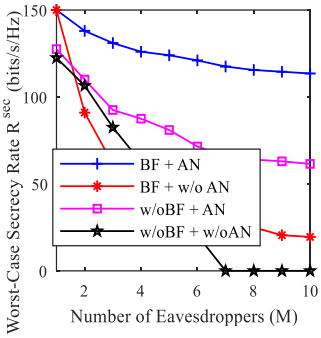

Fig.8. Worst case secrecy rate against number of eavesdroppers

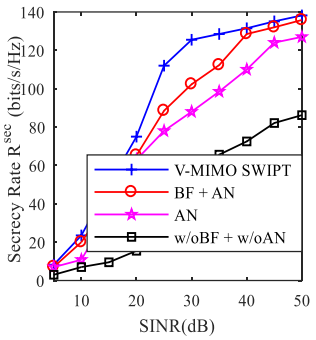

Fig.9. Comparison of secrecy rate over SINR

G. Robustness of the Proposed Scheme as Worst-Case Secrecy Rate Over Increasing Number of Eavesdropper

Fig. 8 shows that, there is reduction in the worst-case secrecy rate with increment of the eavesdroppers (M) in all the schemes. It can be observed that the proposed scheme with beamforming and injected artificial noise (BF+AN) is much robust, and it does not lower down the secrecy rate too much compare to others schemes. Whereas, the second scheme with beamforming but without artificial noise (BF+w/oAN) secrecy rate drops quickly, because there is information leakage as there are no jamming nodes which insert artificial noise to produce distortion at eavesdropper's channel. The third scheme, without beamforming but have artificial noise (w/o BF+AN) achieve better secrecy rate than (BF+w/oAN). This is due to the reason that as the eavesdroppers' number increases, AN has more influence to block the information leakage in spite of BF. Finally, the traditional scheme without beamforming and without artificial noise (w/oBF+w/oAN) achieves worst secrecy rate performance and reaches to zero at $M = 7$. Thus, it is analyzed that the proposed scheme keep system secrecy rate 55%, 95% and 110% higher than w/o BF+AN, BF+w/oAN and w/oBF+w/oAN respectively, which proved the robustness of proposed scheme under different number of eavesdroppers The reason is that artificial noise affects the SINR negatively at the eavesdropper, which in turn improves the secrecy rate between the transmitting node and the authorized receiving node.

H. Robustness of System Secrecy Rate Over Received Value of SINR at Receiver Side

Fig. 9 demonstrates the comparative analysis of the system secrecy rate against different SINR values and shows the robustness of the proposed secure V-MIMO SWIPT technique against the state-of-the-art schemes. It can be analyzed from the result that increasing value of SINR at the receiving node enhances the secrecy rate in all the schemes. Further, it is clear from the result that the scheme which has not used beamforming and artificial noise (w/oBF+w/oAN) for PLS has worst system secrecy rate in contrast to the scheme which has used only AN technique to provide security in the network [9]. However, the scheme which has employed both beamforming and artificial noise technique (BF+AN) [16] has better performance than the other two schemes i.e., (w/oBF+w/oAN) and (AN). In the proposed scheme secrecy rate is far better (about 70%) than traditional scheme (w/oBF+w/oAN). Further, in the proposed scheme secrecy rate improves 15-20% and 22-27% in the range of SINR (40 to 50 dB) against the scheme enabled with BF+AN and only with AN respectively. This is because the proposed scheme uses additional V-MIMO SWIPT technique, which enables the spatial diversity and improves the information decoding rate than other schemes.

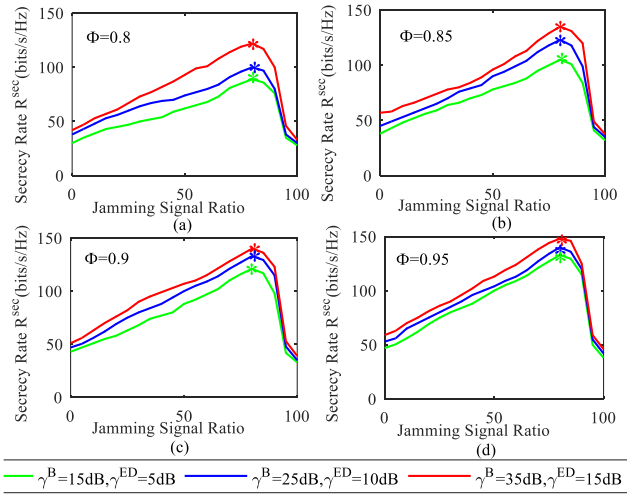

Fig.10. Secrecy rate over JSR (a) Φ = .8 (b) Φ = .85 (c) Φ = .9 (d) Φ = .95.

I. Secrecy Rate Performance with Instantaneous SINR

Fig.10 (a-d) demonstrates the secrecy rate performance of the proposed secure V-MIMO SWIPT technique for different $\Phi = \{0.8, 0.85, 0.9, 0.95\}$ (in the proposed technique eavesdropper is able to cancel out only upto 20% of jamming signals) and over jamming signal ratio (JSR), which is defined as $P_J/(P + P_J)$ under different γ^B, γ^{Ed}. It can be clearly observed from the results, with increasing value of Φ, the secrecy rate also enhances with increase in $\gamma^B (\geq \gamma^{min}(15dB))$ at receiver over increasing JSR. This is because, increment in Φ indicates that eavesdropper cancellation capability of interference decreases and increase in γ^B helps receiver in decoding the received secured message more successfully, which ultimately enhances the secrecy rate. As, $\Phi = 0$ shows perfect interference cancellation (jamming signal) by eavesdropper, which means eavesdropper is able to listen the secured message. On the other hand, even in the increase of γ^{Ed} up to $\gamma^{min} (\leq 15\ dB)$, the secrecy rate seldom changes. This is because jamming nodes of receiver side create strong interference at the eavesdropper side, and eavesdropper does not know both the CSI between receiver and itself, and the structured code of jamming signals, thus it

is not able to mitigate the interference. If the γ^{Ed} is beyond the $15\,dB$ then secured massage is listened by eavesdropper, which indicates the failure of system. It can also be noted down from the results that secrecy rate increases up to optimal point (star (*) marker) with the increment of JSR after that there is considerable degradation in secrecy rate performance. This is because, higher value of JSR indicates strong interference at the receiver itself, and receiver exhausts more power in cancelling out the effect of interference. Thus, less power remains for successful decoding of received secure message; consequently, there is sharp degradation in secrecy rate.

J. Secrecy Region Over Residual Interference Ratio

Fig. 11 (a-b) illustrate the secrecy region of the proposed secure V-MIMO SWIPT technique for different $\Phi = \{0.8, 0.9\}$ with respect to location of the transmitting cluster head 'A' at (0, 0) and receiving cluster head 'B' at (2, 2). The secrecy region is divided into seven vulnerable regions as shown in colorbar. Dark shading (blue) shows less secure region, i.e., more prone to eavesdropping labelled as highest and light shading (yellow) shows more secure region, i.e., less possibility of eavesdropping labelled as lowest.

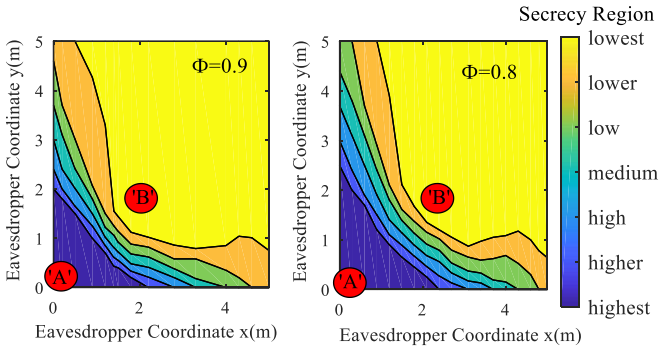

Fig.11. Secrecy region over Eavesdropper location (a) $\Phi = 0.9$ (b) $\Phi = 0.8$

It can be clearly observed that, shading of secrecy region is fade out as the eavesdropper '*e*' moves away from the transmitting cluster head 'A'. This is because, 'B' transmits the jamming signal and the secured information is transmitted by 'A', so when eavesdropper '*e*' is closer to 'B' it is more affected by the jamming signals and subsequently there is decrease in possibility of eavesdropping, which ultimately enhances the achievable secrecy rate and *vice-versa*. Light shading region defines the higher value of secrecy rate, i.e., eavesdropper is unsuccessful in intercepting the main channel,$P(\gamma^{Ed} \leq \gamma^{min})$ and receiver successfully decodes the secured message, $P(\gamma^{B} \geq \gamma^{min})$ corresponds to section III-D. Further, it is also observed that higher value of residual interference ratio also helps in increasing the secrecy rate performance.

VI. CONCLUSIONS

In this paper, a novel secure V-MIMO SWIPT technique is presented for optimizing the secrecy rate of the 5G centric sensors-enabled IoT network. It focuses on the crucial requirements of the network, such as security, reliability and energy efficiency. In this regard, a maximization problem is formulated in order to maximize the secrecy rate by collectively optimizing the beamforming vector, the PS ratio and the TS ratio. Since the problem is non-convex, to find the solution of the problem an iterative algorithm is presented. Penalty function method is used to develop the solution. The proposed technique is proved to be more effective as compared the state-of-the-art schemes by simulations. The proposed work is limited to OMA transmission mode in wireless sensors enabled IoT network. Also, use of beamforming technique requires CSI before the start of transmission. In this paper, transmitter knows the CSI by the received feedback message from receiver. In future research, the proposed work will be extended to cognitive radio network to secure transmission in the presence of active eavesdropper with dynamic CSI for secrecy rate maximization.

REFERENCES

[1]. Asif-Ur-Rahman, M., Afsana, F., Mahmud, M., Kaiser, M.S., Ahmed, M.R., Kaiwartya, O. James-Taylor, A.,Toward a heterogeneous mist, fog, and cloud-based framework for the internet of healthcare things. IEEE Internet of Things Journal, 6(3), pp.4049-4062, 2018.

[2]. Makarfi, A.U., Rabie, K.M., Kaiwartya, O., Adhikari, K., Nauryzbayev, G., Li, X. and Kharel, R., Towards Physical Layer Security for Internet of Vehicles: Interference Aware Modelling. IEEE Internet of Things Journal, PP. 1-22, 2020. (Online Published)

[3]. Budhiraja, I., Kumar, N., Tyagi, S., Tanwar, S. and Guizani, M., An Energy-Efficient Resource Allocation Scheme for SWIPT-NOMA based Femtocells users with Imperfect CSI. IEEE Transactions on Vehicular Technology, 69(7), pp. 7790-7805, 2020.

[4]. M. Alageli, A. Ikhlef and J. Chambers, "SWIPT Massive MIMO Systems With Active Eavesdropping," in IEEE Journal on Selected Areas in Communications, vol. 37, no. 1, pp. 233-247, 2019.

[5]. Budhiraja, I., Tyagi, S., Tanwar, S., Kumar, N. and Rodrigues, J.J., Tactile Internet for smart communities in 5G: An insight for NOMA-based solutions. IEEE Transactions on Industrial Informatics, 15(5), pp.3104-3112, 2019.

[6]. P. Huang, Y. Hao, T. Lv, Xing, J., J. Yang, P. T. Mathiopoulos, "Secure Beamforming Design in Relay-Assisted Internet of Things," IEEE Internet of Things Journal, pp. 6453-6465 ,2019.

[7]. Kumar, S., Singh, K., Kumar, S., Kaiwartya, O., Cao, Y., Zhou, H., Delimitated anti jammer scheme for Internet of vehicle: Machine learning based security approach, IEEE Access, 7, 113311-113323, 2019

[8]. Zeng, M., Yadav, A., Dobre, O.A., Tsiropoulos, G.I. and Poor, H.V., 2017. Capacity comparison between MIMO-NOMA and MIMO-OMA with multiple users in a cluster. IEEE Journal on Selected Areas in Communications, 35(10), pp.2413-2424, 2017.

[9]. Verma, G.K., Singh, B.B., Kumar, N., Kaiwartya, O., Obaidat, M.S., PFCBAS: Pairing Free and Provable Certificate-Based Aggregate Signature Scheme for the e-Healthcare Monitoring System. IEEE Systems Journal, 14(2), 1704-1715, 2020.

[10]. Kumar, S., Kaiwartya, O., Rathee, M., Kumar, N. and Lloret, J., Toward Energy-Oriented Optimization for Green Communication in Sensor Enabled IoT Environments. IEEE Systems Journal, 2020. (online published) DOI:10.1109/JSYST.2020.2975823

[11]. J. Qiao, H. Zhang, X. Zhou and D. Yuan, "Joint Beamforming and Time Switching Design for Secrecy Rate Maximization in Wireless-Powered FD Relay Systems," IEEE Transactions on Vehicular Technology, vol. 67, no. 1, pp. 567-579, Jan. 2018.

[12]. H. Zhang, H. Xing, J. Cheng, A. Nallanathan, and V. C. Leung, "Secure resource allocation for OFDMA two-way relay wireless sensor networks without and with cooperative jamming," IEEE Transactions on Industrial Informatics, vol. 12, no. 5, pp. 1714–1725, 2016.

[13]. L. Lv, Z. Ding, Q. Ni and J. Chen, "Secure MISO-NOMA Transmission with Artificial Noise," IEEE Transactions on Vehicular Technology, vol. 67, no. 7, pp. 6700-6705, July 2018.

[14]. A. Alsadi and S. Mohan, "Improving the Physical Layer Security of the Internet of Things (IoT)," IEEE International Smart Cities Conference (ISC2), Kansas City, MO, USA, pp. 1-8, 2018.

[15]. H. Zhang, H. Xing, J. Cheng, A. Nallanathan, and V. C. Leung, "Secure resource allocation for OFDMA two-way relay wireless sensor networks without and with cooperative jamming," IEEE Transactions on Industrial Informatics, vol. 12, no. 5, pp. 1714–1725, 2016.

[16]. 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 Journal on Selected Areas in Communications, vol. 36, no. 4, pp. 918-931, April 2018.
[17]. L. Lv, Z. Ding, Q. Ni and J. Chen, “Secure MISO-NOMA Transmission with Artificial Noise,” IEEE Transactions on Vehicular Technology, vol. 67, no. 7, pp. 6700-6705, July 2018
[18]. M. Zhang and Y. Liu, “Secure Beamforming for Untrusted MISO Cognitive Radio Networks,” IEEE Transactions on Wireless Communications, vol. 17, no. 7, pp. 4861-4872, July 2018.
[19]. M. Zhao, S. Feng, X. Wang, M. Zhang, Y. Liu and H. Fu, “Joint Power Splitting and Secure Beamforming Design in the Wireless-Powered Untrusted Relay Networks,” *2015* IEEE Global Communications Conference (GLOBECOM), San Diego, CA, pp. 1-6, 2015.
[20]. V. NhanVo, D. Tran, C. So-In and H. Tran, “Secrecy Performance Analysis for Fixed-Gain Energy Harvesting in an Internet of Things with Untrusted Relays,” IEEE Access, vol. 6, pp. 48247-48258, 2018.
[21]. H. Xing, K. Wong, Z. Chu & A. Nallanathan, “To Harvest and Jam: A Paradigm of Self-Sustaining Friendly Jammers for Secure AF Relaying,” IEEE TransactionsSignal Processing, vol. 63(24), pp. 6616-6631, 2015.
[22]. K. Wang, L. Yuan, T. Miyazaki, D. Zeng, S. Guo, & Y. Sun, “Strategic anti-eavesdropping game for physical layer security in wireless cooperative networks,” IEEE Transactions on Vehicular Technology, 66(10), pp. 9448-9457, 2017.
[23]. K. Moara-Nkwe, Q. Shi, G. M. Lee, & M. H. Eiza, “A novel physical layer secure key generation and refreshment scheme for wireless sensor networks,” IEEE Access, 6, pp. 11374-11387, 2018.
[24]. K. Hamsha and G. S. Nagaraja, "Analysis of security mechanism using threshold cryptography for hierarchical wireless sensor networks," 2017 International Conference on Communication and Signal Processing (ICCSP), Chennai, 2017, pp. 1938-1941.
[25]. S. Han, H. Kim, J. Lee and J. Choi, "Secure Capacity Analysis for Magnetic Inductive Coupling-Based SWIPT System," in IEEE Access, vol. 6, pp. 49182-49191, 2018.
[26]. T. T. Tran and H. Y. Kong, "CSI-Secured Orthogonal Jamming Method for Wireless Physical Layer Security," in IEEE Communications Letters, vol. 18, no. 5, pp. 841-844, May 2014.
[27]. X. He, A. Yener, Providing secrecy with structured codes: Two-user Gaussian channels, IEEE Trans. Inf. Theory, 60(4), 2121–2138, 2014.
[28]. K. Anoh, G. Okorfor, B. Adebisi, A. Alabdullah, S. Jones, R.Alhameed, "Full-Diversity QO-STBC Technique for Large-Antenna MIMO Systems", *Electronics (MDPI)*, vol. 6, no. 2, 2017.
[29]. M. V. Dolgopolik “Exact penalty functions for optimal control problems II: Exact penalization of terminal and pointwise state constraints” Wiley, vol. 41, Issue 3, pp.898-947, Jan 2020.
[30]. Bansal, A., Kaiwartya, O., Singh, R.K. and Prakash, S., Maximizing fault tolerance and minimizing delay in virtual network embedding using NSGA-II. In Proc. of the Third International Symposium on Women in Computing and Informatics (pp. 124-130), 2015.