Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 4, 2021, Pages. 4179 - 4190
Received 05 March 2021; Accepted 01 April 2021.

Cognitive Radio-Based IoMT with Wireless Energy Harvesting for Secure Transmissions

[1]A.Prabhu, [2]R.Raja, [3]P.Manikanda Prabu, [4]P.Dinesh,[5]S.Manimekalai

[1]AssistantProfessor,Departmentof EEE, K.Ramakrishnan College of Engineering,Tiruchirapalli,Tamilnadu.Email:prabhumepse@gmail.com

[2]Assistant Professor, Department of MCA, AnjalaiAmmalMahalingamEngineering College, Tiruvarur,Tamilnadu. Email:miltonraja@gmail.com

[3]Assistant Professor, Department of CSE, AnjalaiAmmalMahalingam Engineering College, Tiruvarur,Tamilnadu. Email:maniadt2006@gmail.com

[4]Assistant Professor, Department of CSE, AnjalaiAmmalMahalingam Engineering College, Tiruvarur, Tamilnadu. Email:dincseinfo@gmail.com

[5]Assistant Professor,PSNA College of Engineeringand Technology, Dindigul,Tamilnadu. Email:manimekalaisuresh06@gmail.com

Abstract

The challenge of safe transmission of the collection of wireless energy to the cognitive Internet of Medical Things (IoMT). The primary-transmitter (PT) can listen to PT sensitive information, if we consider the potential eavesdropper and transmit sensitive medical information through a multi-antenna secondary transmitter to the secondary Transmitter (ST). The ST also sends its personaldata simultaneously through spectrum sharing. The energy-restricted cooperativescheme will be equated to the cooperative scheme without energy restrictions and the non-cooperative energy-restricted system in this studying. The energy Harvesting (EH) ratio and secures beamforming are proposed as branch-reduceand-bound (BRB). Furthermore, the conditions are specified for the system to switch from cooperative to non-cooperative modes. To make simpler research, a dominant system method is used to achieve a closed communication in the scheme's stable throughput field. Also note that, compared with the conventional system, the proposed system model protocol considered will encourage the primary secrecy transmission rate and guarantee the transmission rate of the subordinatescheme.

KEYWORD: Internet of Medical Things, cognitive radio, energy-constrained cooperative system and medical data.

1 Introduction

IoMT is a global facility for the collection of information technology (IT)-based medical devices and applications [1-3]. In addition, IoMT is called IoT medicine. IoMT uses an accelerometer, visual sensor, Co2 sensor, ECG/EMG sensors, gyroscope sensor, humidity sensor, respiratory sensors,saturation blood oxygen sample, and a blood pressure sensor for continuous monitoring and monitoring of patients' wellbeing. The IoMT senses patients'condition and then transfers medical data to doctors and caregivers via the remote

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 4, 2021, Pages. 4179 - 4190
Received 05 March 2021; Accepted 01 April 2021.

cloud datacentre [4, 5]. These data are used most often for diagnostic and medical treatment purposes.

The useful data collected from the medical record are used to avoid and protect patients' health in emergency situations. The key difficulty in IoMT though is to deal with vital applications for vast amounts of medical data from different associated devices [6, 7]. This huge size of data was often called enormous data that cannot be treated with obsolete procedures and applications. Intelligent investigation and the collection of large quantities of medical data allow IoMT to increase prudence and the diagnosis of early diseases. Scalable learning and smart algorithms, leading to more interoperable solutions and active choices for emerging IoMTs, are thus needed nowadays.

According to a study carried out by the related organisations, the marketplace for IoMT will range about US$117 by the end of 2020[8]. However, with the increased use of IoMT devices, the huge claim for radio spectrum poses serious problems. In adding, the permitted radio spectrum is often underused due to the fixed spectrum policy[9]. There has been a cognitive radio technology which makes it possible to use spectrum resources efficiently, i.e. allowing unlicensed nodes, without impairing primary broadcasts, to transmit each other opportunistically through licensed frequency bands[10-12].

However, power supply also impedes the growth of IoMT. In universal, an IoMT system needs various small battery-operated devices that are problematic to substitute. This is a problem that has gained considerable attention from wireless technology. Energy harvesting (EH) devices can relay data from the atmosphere for sun, wind and RF signals[13]. Data can be converted from the surrounding environment. Wireless EH was more drawn to its advantages and in particular to its RF signals for wireless, inexpensive, and short form execution in the development of circuit systems synchronously. The energy collected is also in the range of thousands of watts required for small power IoMT devices such as small distance health data sensors. Therefore, by incorporating EH in cognitive radials, both the spectrum and energy effectiveness of medical WSN can be improved.

Although IoMT transfer effectively improves the efficiency of cognitive EH radio technology, many safety issues are faced with a number of medical devices [17]. Given that stringent sensors need energy collection and then wireless transmission of sensitive data to patients, other sensors may be able to eavesdropper such confidential communications [18]. In a number of applications, several health care professionals develop and are ready to use IoT technology without taking security into account. This leads to new privacy, honesty and availability issues. Furthermore various IoMT sensors are not able to integrate the encryption procedure due to their partial capacity, such as lack of operational measurement and adequate energy supply. Thus it is simple to find and exploit this absence of robust encryption via medical sensors.

2 Literature review

Relay selection is an effective solution for safe secondary user knowledge transmission against EH cognitive networks. Increasing the incorporation of SWIPT and

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 4, 2021, Pages. 4179 - 4190
Received 05 March 2021; Accepted 01 April 2021.

Cooperative Relay (CoR) methods has emerged as a noveloccurrence for a WSN of the next century. CoR is used to get a power and effective spectral network to resolve the problems of fading, loss of trajectory, shade and smaller areas. Battery-restricted or battery-less equipment are relay nodes. Often, they need external charging devices that are not feasible and convenient to replace or recharge their batteries. EH is the effective in cost, appropriate and safer way to power these relays. SWIPT is the most important technology, among different types of EH, as it offers spectral efficacy by simultaneously supplying energy and data to the relays.

SWIPT and CoR are encouraged to deliver EE and SE with NGWN. In recent years, technology like 5G, huge IoT, and other emerging tools have become one of the most critical issues, and are constantly complex in terms of architecture, cost and power[19]. Due to the widespread development of various applications, the energy use of networking devices has improved exponentially. In 2025, IoT devices are projected to rise almost 26 to 46 billion according to the Bell Labor Gartner and Cisco[20]. Numerous batteries are needed and thousands of IoT devices need to be saved and disposed of properly. The global IT sector consumed 616 TWh of electricity in 2013 and is predicted to expand by the year 2020 to 910 TWh[21]. It is also projected that by 2025 the annual emissions of carbon will range up to 235 M [22-23]. This troubling situation poses significant problems for researchers with low energy use and carbon emissions. These batteries must be properly stored and eliminated to enhance the environment. For the SWIPT co-operative relays network, this can be a promising option.

There has been extensive research on SWIPT and CoR integration in latest years with practical benefits and solutions for numerousdifficulties and opportunities for research. The inclusion of both SWIPT and CoR is studied and addressed separately in many journals. As far as we are aware, there is no detailed survey of SWIPT and CoR's integrated aspects and their implementation in the next generation framework.

3 System Model and Transmission Protocol

We interpret a Wireless Relay Cognitive Network as shown in Figure 1. PT and primary receiver (PR) are the main system, while the secondary system is a ST and secondary receiver (SR). A new eavesdropper (ME) is also available for the purpose of intercepting the confidential data of the PT in a primary scheme in which PT plans to send trusted information to PR. The primary scheme may be considered as the connection between a low channel quality or a lower speed transmission system. The ST is therefore ready to serve as a relay for the supply of its own data to primary communication. We accept that the PT has a stationary supply of power while the ST has partial battery capacity, so the received RF signal requires energy. The ST features N antennas, while other nodes work with a single antenna in a semi-duplex mode.

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 4, 2021, Pages. 4179 - 4190
Received 05 March 2021; Accepted 01 April 2021.

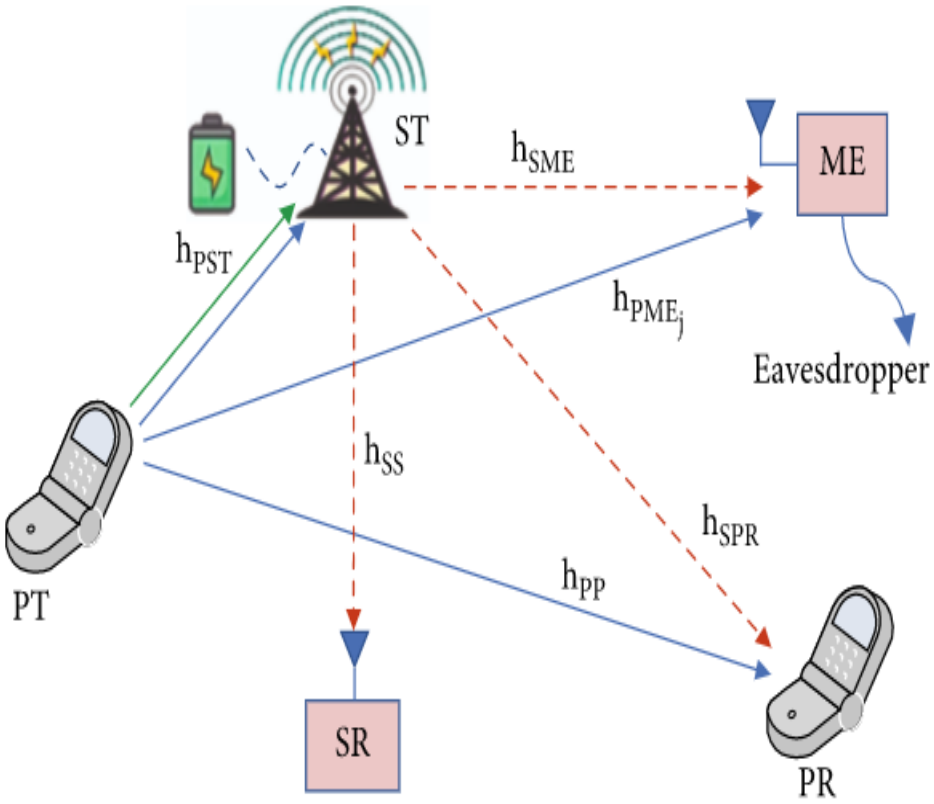

Figure 1:The CRN-WPR system model.

All channels are subject to the flat block of the Rayleigh fading channel, which slot and self-governing shift in separate transmission slots is characterised by quasistatic channel status. Let h_{PST}, h_{SSS}, h_{SME},and h_{SPR} be the compound channel vectors of the ST-SR, ST-ME,PT-ST, and ST-PR, correspondingly.

4 Information Transmission and Energy Harvesting

The EH and transmission of information in one transmission slot include three stages as shown in Figure 1. In the first point, the PT is transmitting the x_e energy signal to the ST for the EH using a portion of time $\alpha[\alpha\epsilon(0,1)]$from a total block time T to ST. The signal obtained at the ST can therefore be expressed as

$$y_{ST}^{I} = \sqrt{P_p h_{PST} x_e + n_{ST}} \tag{1}$$

where P_p signifies the transmission node power PT, x_e signifies the energyunit-power signal, and $n_{ST}\sim n(\delta_{ST} I)$is the expectedAWGN with variance ofδ_{ST} . We assume T=1 for definitivity and no loss of generality. The sum of HE at the ST can therefore be estimated as

$$E_{ST} = \alpha\eta P_P \|h_{PST}\|^2 \tag{2}$$

where $\eta\varepsilon[0,1]$ is efficiency of energy transformation.Note that the sum of scavenged noise energy is ignored as the thermal noise energy derived can be insignificant compared to the energy signal.

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 4, 2021, Pages. 4179 - 4190
Received 05 March 2021; Accepted 01 April 2021.

At the second stage of duration $(1-\alpha)T/2$, the PT transmits stable signal x_p with power , $P_P$the received sign at the ST is thus given as

$$y_{ST}^{II} = \sqrt{P_p h_{PST} x_P + n_{ST}} \tag{3}$$

The attainable rate R_{ST}can be resulting as

$$R_{ST} = \frac{(1-\alpha)T}{2} Log_2\left(1 + \frac{P_P \|h_{PST}\|^2}{\delta_{ST}}\right) \tag{4}$$

Because of the essence of the info transmitted, the PR and the eavesdropper ME may also receive a signalx_p.

$$y_{PR}^{II} = \sqrt{P_p h_{PP} x_P + n_{PR}} \tag{5}$$

$$y_{ME}^{II} = \sqrt{P_p h_{PME} x_P + n_{ME}} \tag{6}$$

During the third phase$n_{PR} \sim n(0, \delta_{PR})$, First, ST node decodes the primary signal $x_P$on DF dependent primary confidential processing receipts, then, by using the beamforming vectors, simultaneously, forward $x_P$and its own $x(s)$ signal. The corresponding signal obtained by the PR and eavesdropper ME is therefore stated as

$$y_{ME}^{III} = h_{SPR}^H v_p x_p + h_{SPR}^H V_S x_S + n_{PR} \tag{7}$$

$$y_{ME}^{III} = h_{SME}^H v_p x_p + h_{SME}^H V_S x_S + n_{PR} \tag{8}$$

The PR tries to retrieve x_p from y_{ME}^{III}in the occurrence of the secondary signal . The eavesdropper would also intercept the $x_P$signal in the meantime. The achieved PR and ME rates can therefore be described in two phases:

$$R_{PR} = \frac{(1-\alpha)T}{2} Log_2\left(1 + \frac{P_P \|h_{PP}\|^2}{\delta_{PR}} + \frac{\left|h_{SPR}^H V_P\right|^2}{\left|h_{SPR}^H V_S\right|^2 + \delta_{PR}}\right) \tag{9}$$

$$R_{ME} = \frac{(1-\alpha)T}{2} Log_2\left(1 + \frac{P_P \|h_{PME}\|^2}{\delta_{ME}} + \frac{\left|h_{SME}^H V_P\right|^2}{\left|h_{SME}^H V_S\right|^2 + \delta_{ME}}\right) \tag{10}$$

At the SR, the received signal is assumed by

$$y_{SR} = h_{SS}^H v_S x_S + h_{SS}^H V_P x_P + n_{SR} \tag{11}$$

Similar to the SR and PR, treats x_P as interfering and then notices the desired x_S. The attainable rate at the SR is given by

$$R_{SR} = \frac{(1-\alpha)T}{2} Log_2\left(1 + \frac{\left|h_{SS}^H V_S\right|^2}{\left|h_{SS}^H V_P\right|^2 + \delta_{SR}}\right) \tag{12}$$

5 Problem Invention and Secure Beamforming

In this division, we first describe the primary system confidentiality rate, which is the crucial performance indices to demonstrate the sensitive data's transmission protection and

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 4, 2021, Pages. 4179 - 4190
Received 05 March 2021; Accepted 01 April 2021.

then express the optimization problem by optimizing the primary privacy rate to meet the minimum possible secondary system and relay ST relay node power constraint. We also suggest a mathematic-efficient optimisation system to solve the difficult with a two-stage process in order to achieve optimum data security parameters efficiently. Two -antenna PUs as (PU 1 and PU 2) in the main network aim to share information on both primary and secondary networks, while the illegal eavesdropper (named Eve) with a single antenna is involved in data from PUs and attempts to link it to wireless connections. A CR-enabled controller and multiple IoDs 1 form a secondary network. The N antenna-equiped controller provides cooperatively stable relay support for the PU and serves primary spectrum for the secondary IoDs, which are at the core of the secondary network. Multiple IoDs work for various functions, in particular, K ID-IoDs for the decoding of basic information and M EH-IoDs for energy collection. One common scenario is the smart home-app, which simultaneously transmitts twice the information and co-operatively secrecy to PUs (e.g. smartphones, laptops or controls in a different subsystem IoT), through an IoT control center, thus using the primary spectrum to send downlink data to its various IoT clients. We concentrate on the design of the safe beam shaping device at the central controller in this research.

In two consecutive time frames, stable information transmission and energy collaboration are separated.In the first slot, PU-1 and PU-2 concurrently transmit symbols $x1 \in C\ 1 \times 1\ and\ x2 \in C\ 1 \times 1$ to the controller with average communicatepower $E[|xi\ |\ 2\ ] = Pi\ , i \in \{1, 2\}$, correspondingly. We signify the forward channel reply from PU i to the controller 2 as hi,$f \in C\ N \times 1$.

Thus, the received signals at the controller and eavesdropper in the first time slot are stated as

$$t_r = h_1, f^{x1} + h_2 f^{x2} + n_r \tag{13}$$

$$y_{e,1} = f_1 x_1 + f_2 x_2 + n_{e,1} \tag{14}$$

where$n_r \sim CN(0, \sigma^2 I)$ and$n_e \sim CN(0, \sigma^2)$refer to the AGN at the controller and the eavesdropper, correspondingly.

Since *I* know its transmitting symbol in (1), when acceptance the reverse signal from the controller it can remove the interference. Thus, the signals received by the PU *I* and the eavesdropper are conveyed next time

$$y_{d,i} = h_{i,b}^T \left(F h_{3-i,fx3-i} + \sum_{j=1}^{K} w_{j3j} + F n_r\right) + n_{d,i} \tag{15}$$

$$y_{e,2} = f_r^T \left(\sum_{p=1}^{2} F\ h_{3-i,fx3-i} + \sum_{j=1}^{K} w_{j3j} + F n_r\right) + n_{e,2} \tag{16}$$

Where, $h_{i,b}, f_r \in N * 1$Denote the retroactive vactors in PU and eavesdropper channel reaction from the controller. $nd, i, n_e \sim CN(0, \sigma^2)$ refers to Gaussian additive noise in PU I and eavesdropper.

Established on (5), the established SINR at PU i can be articulated as fractional quadratic form as

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 4, 2021, Pages. 4179 - 4190
Received 05 March 2021; Accepted 01 April 2021.

$$\gamma i = \frac{fB_i f}{fB_i f + \sum_{j=1}^{K} W_j C_i W_j + \sigma^2} \quad (17)$$

Our goal is to optimize the secrecy of PUs under the control controller transmission power constraint and the SINR, EH, and beamforming$F$ series at each IoT, through optimisation W_j.

6 BRB-BASED ITERATIVE ALGORITHM

The problem of secrecy summary maximization (18) is a quadratic quadratic non-convex programming problem (FQCQP) and it is thus trying to get an optimum solution using traditional convex methods. We will suggest an iterative algorithm BRB technique in this section to provide a reference point for evaluating a problem associated to other suboptimal procedures (19). The principle of the BRB-based approach proposed is to remediately update a number of uncut boxes and to reduce the box size continuously, thereby driving the objective value into the optimal. In particular, the BRB algorithm proposed involves three steps: branch, reduction and bound. Proposed SSR Maximization Problem BRB based esterative algorithm (20).

First, the box set N = {m0}, which includes the original box M0 = [a0, b0], is initialized. The objective problem function (20) can be simplified by dismissing the logarithm term for determining the size of M0 in a product shape.that is, R¯ s = f(γ) = γ1γ2γ3 , where

$$\gamma_i = 1 + \frac{fB_i f}{fR_i f + \sum_{j=1}^{K} W_j C_i W_j + \sigma^2} \quad (18)$$

$$\gamma_3 = \frac{\sigma^4 (1 + fB_i f) + \sigma^2 \sum_{j=1}^{K} W_j C_i W_j}{fR_4 f + \sum_{j=1}^{K} W_j C_4 W_j + \beta} \quad (19)$$

Particularly,$b_0 = [\gamma_i, max\gamma_2, max, \gamma_3, , max]\, T$ is the upper right vertex selected as a vector containing of the maximal values of γ_i, γ_2, γ_3, and $a_0 = [\gamma_i, max\gamma_2, max, \gamma_3, , max]\, T$ is the lower left vertex created by the least values of γ_i, γ_2, γ_3.

Based on the expressions in (21),γ_i, γ_2, γ_3.are generalized forms of Rayleigh quotients with a maximum value of the widespread matrices. The higher and lower limits are thereforeof γ_i, γ_2, γ_3.are listed below,

$$\gamma_i, min = 1, \gamma_i, max = 1 + \frac{P_r}{\sigma^2 \lambda_{max}\,(A^{-1} B_i)}, i = 1,2$$

$$\gamma_2, min = \frac{\sigma^4}{\beta} + P_r / \beta \lambda_{max}\,, (M^{-1}, X) \quad (20)$$

$$\gamma_3, min = \frac{1}{\beta} + P_r / \beta \lambda_{max}\,, (M^{-1}, Y) \quad (21)$$

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 4, 2021, Pages. 4179 - 4190
Received 05 March 2021; Accepted 01 April 2021.

The BRB-based Iterative Procedure

Step.1: original box input as M0 = [x0, y0], the box set N = {M0}, accuracy as ε and division line search accuracy as δ;

Step. 2: Set initial fmin and fmax;

Step.3: while fmax − fmin> ε

Step.4: select the box M = [x, y] with feasible lower point y and f(x) = fmax;

Step.5: while 1 First-rate a box [a, y] with f(b) = fmax from N ; Checked the feasibility of; [x, y] is selected; break else: eliminate the box from the and update the upper bound $fmax\ as\ fmax\ =\ arg\ max[x, y] \in N$ f(b); end

end

7 SIMULATION RESULTS

In this division, we shall verify the safety presentation of the primary system transmission and the subordinate system transmission efficiency by comparing the system and ZF-based system proposed. We accept that all noise capacity is uniform, unless otherwise specified,i.e.,$\delta_{PR} = \delta_{SR} = \delta_{ME} = 1$. The distance from PT to PR is 8 m, the distance from ST to SR is 3 m. We also take into account a scenario. In addition, 4 antennas are provided for the ST and η=0.5 is determined for efficiency in energy harvesting.

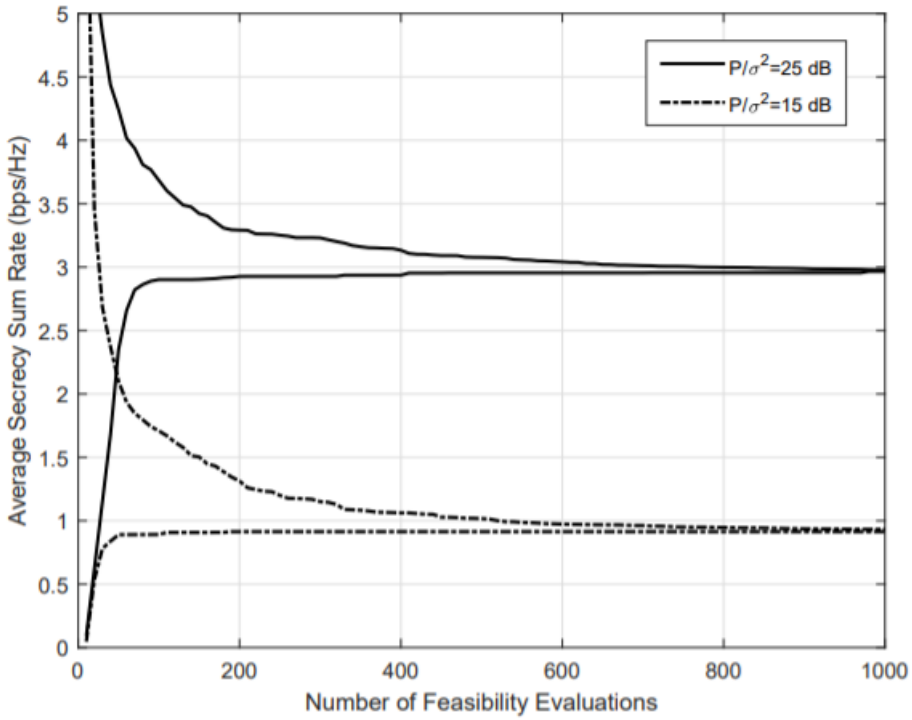

Fig. 2. Average secrecy sum rate versus the sum of feasibility assessments in the BRB- algorithm

In the picture. 2, we display the average BRB-based iterative algorithm secrecy sum rate versus the total amount of feasibility assessments. The number of antennas is N = 3 and

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 4, 2021, Pages. 4179 - 4190
Received 05 March 2021; Accepted 01 April 2021.

the power ratio from transmission to sound is Pr/4-02 = 25 dB. A line-search accuracy α = 0.01 is applied to the bisection method; the termination precise is μ = 0.1.

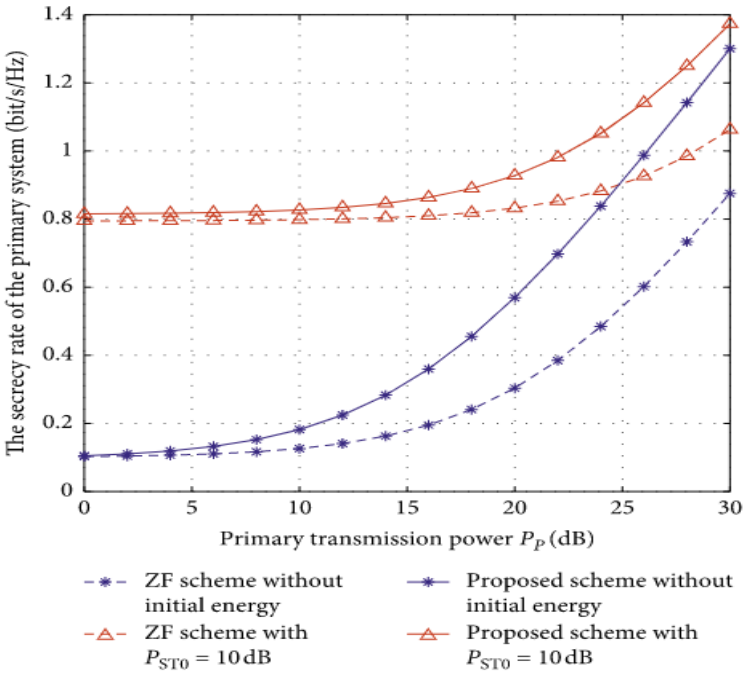

Figure 3.The secrecy rate of the PS with detail to the P_P for diverse initial energies at the ST.

Figure 3 shows the primary system secrecy rates for primary transmission power in various initial ST energies. In this figure, with increasing primary transmission power the secrecy rates of the PS with the projected scheme and the ZF regime are increased.

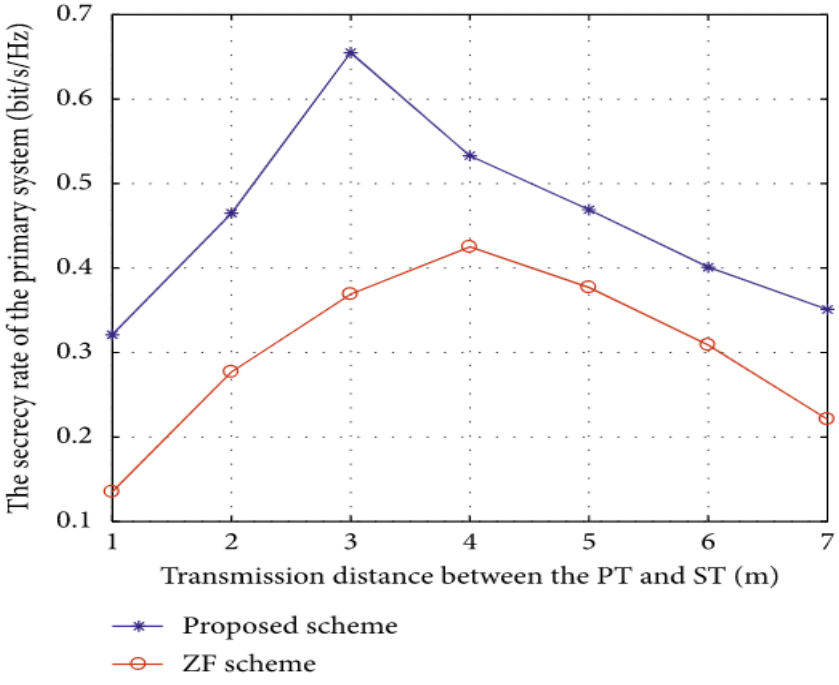

Figure 4: The secrecy rate of the distance between the PT and ST.

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 4, 2021, Pages. 4179 - 4190
Received 05 March 2021; Accepted 01 April 2021.

The secrecy rates between the PT and ST under the proposal and the ZF method are shown in Figure 4. This figure shows that the projectedsystem is greater to the ZF system in respect of primary secrecy regardless of where the ST stands.The rise in d_{PST} first increases and then worsens primary secrecy rates. The d_{PST} secrecy rate is increased when the transmission distance is low, when the d_{PST} increase, as more energy is collected so as to transmit the signal and shorter distances for the transmission of the primary signal. If the d_{PST} distance is longer, the secrecy rate deteriorates because it helps the ST to transmit the signal of the TP by means of the amount of energy obtained and by further path loss. Moreover, the ST positions can be guaranteed for the proposed scheme and ZF scheme at approximately 3 m and 4 m respectively.

8 Conclusions

This paper discussed the protection issue of the cognitive radioactive IoMT transmission when a malicious eavesdropper listens to the sensitive medical facts sent from PT. We express the corresponding problematicto safeguard the protection of sensitive data and propose a revolutionary algorithm to design the optimal EH length along with stable beamforming vectors, to optimize the primary transmission secrecy rate and ensure the transfer requirements of the secondary device. Indeed, more than one can be generally used in the eavesdropper, and optimized beamforcing vectors can still be obtained via the proposal. The numerical findings provide excellent safe transmission efficiency with the proposed system, which can be deployed into the IoMTstrategies to guard the protection of sensitive data effectively.

References

[1]. Manogaran G, Lopez D (2018) Spatial cumulative sum algorithm with big data analytics for climate change detection. ComputElectrEng 65:207–221.

[2]. Manogaran G, Varatharajan R, Lopez D, Kumar PM, Sundarasekar R, Thota C (2018) A new architecture of Internet of Things and big data ecosystem for secured smart healthcare monitoring and alerting system. FuturGenerComputSyst 82:375–387

[3]. Manogaran G, Varatharajan R, Priyan MK (2018) Hybrid recommendation system for heart disease diagnosis based on multiple kernel learning with adaptive neuro-fuzzy inference system. Multimedia tools and applications 77(4):4379–4399

[4]. Manogaran G, Vijayakumar V, Varatharajan R, Kumar PM, Sundarasekar R, Hsu CH (2017) Machine learning based big data processing framework for cancer diagnosis using hidden Markov model and GM clustering. WirelPersCommun 1–18.

[5]. Manogaran G, Lopez D (2017) A Gaussian process based big data processing framework in cluster computing environment. ClustComput 1–16.

[6]. Manogaran G, Lopez D, Chilamkurti N (2018) In-Mapper combiner based MapReduce algorithm for processing of big climate data. FuturGenerComputSyst 86:433–445.

[7]. Gafar MG, Elhoseny M, Gunasekaran M (2018) Modelingneutrosophic variables based on particle swarm optimization and information theory measures for forest fires. J Supercomput 1-18.

[8]. F. Alsubaei, S. Shiva, and A. Abuhussein, "Security and privacy in the internet of medical things: taxonomy and risk assessment," in Proceedings of the 42nd IEEE Conference on Local Computer Networks Workshops, pp. 112–120, Banff, Canada, July 2015.

[9]. Federal Communications Comission, In the Matter of Unlicensed Operation in the TV Broadcast Bands: Second Report and Order and Memorandum Opinion and Order, FCC, Washington, DC, USA, 2008.

[10]. M. Sharma and A. Sahoo, "Stochastic model based opportunistic channel access in dynamic spectrum access networks," IEEE Transactions on Mobile Computing, vol. 13, no. 7, pp. 1625–1639, 2014.

[11]. N. Zhang, H. Liang, N. Cheng, Y. Tang, J. W. Mark, and X. S. Shen, "Dynamic spectrum access in multi-channel cognitive radio networks," IEEE Journal on Selected Areas in Communications, vol. 32, no. 11, pp. 2053–2064, 2014.

[12]. D. Jiang, Y. Wang, C. Yao, and Y. Han, "An effective dynamic spectrum access algorithm for multi-hop cognitive wireless networks," Computer Networks, vol. 84, pp. 1–16, 2015.

[13]. C. Han, J. Li, Y. Yang, and F. Ye, "Combining solar energy harvesting with wireless charging for hybrid wireless sensor networks," IEEE Transactions on Mobile Computing, vol. 17, no. 3, pp. 560–576, 2018.

[14]. I. Ahmed, M. M. Butt, C. Psomas, and A. Mohamed, I. Krikidis and M. Guizani, Survey on energy harvesting wireless communications: challenges and opportunities for radio resource allocation," Computer Networks, vol. 88, pp. 234–248, 2015.

[15]. H. Chen, C. Zhai, Y. Li, and B. Vucetic, "Cooperative strategies for wireless-powered communications: an overview," IEEE Wireless Communications, vol. 25, no. 4, pp. 112–119, 2018.

[16]. K. Tang, R. Shi, and J. Dong, ",Roughput analysis of cognitive wireless acoustic sensor networks with energy harvesting," Future Generation Computer Systems, vol. 86, pp. 1218–1227, 2018.

[17]. Y. Zhang, C. Xu, X. Lin, and S. Shen, "Blockchain-based public integrity verification for cloud storage against procrastinating auditors," IEEE Transactions on Cloud Computing, 2019.

[18]. Mamta and S. Prakash, "An overview of healthcare perspective based security issues in wireless sensor networks," in Proceedings of the 3rd International Conference on Computing for Sustainable Global Development, pp. 870–875, New Delhi, India, 2016.

[19]. C. Zhang, W. Ahn, Y. Zhang, and B. R. Childers, ''Live code update for IoT devices in energy harvesting environments,'' in *Proc. 5th Non-Volatile Memory Syst. Appl. Symp. (NVMSA)*, Aug. 2016, pp. 1–6.

[20]. M. K. Weldon, *The Future X Network: A Bell Labs Perspective*. Boca Raton, FL, USA: CRC Press, 2016.

[21]. *World Energy Outlook*. Accessed: 2014. [Online]. Available: https://www.iea.org/publications/freepublications/publication/WEO2014.pdf

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 4, 2021, Pages. 4179 - 4190
Received 05 March 2021; Accepted 01 April 2021.

[22]. Y. Mao, J. Zhang, and K. B. Letaief, ‘‘A Lyapunov optimization approach for green cellular networks with hybrid energy supplies,’’ *IEEE J. Sel. Areas Commun.*, vol. 33, no. 12, pp. 2463–2477, Dec. 2015.

[23]. A. Fehske, G. Fettweis, J. Malmodin, and G. Biczok,‘‘The global footprint of mobile communications: The ecological and economic perspective,’’ *IEEE Commun. Mag.*, vol. 49, no. 8, pp. 55–62, Aug. 2011.