J. Sustain. Wireless Syst., vol. 03, no. 2, pp. 107-117
https://doi.org/10.36548/jsws.2021.2.005

Modified Backscatter Communication Model for Wireless Communication Network Applications

Dr. Joy Iong Zong Chen
Professor,
Department of Electrical Engineering,
Da-Yeh University,
Changhua County, Taiwan.

Abstract: The green communication and large-scale connection issues will be faced by the wireless communication networks with futuristic sixth generation (6G) technology. The radio-frequency (RF) and spectrum sources may be shared simultaneously to achieve optimal communication in these networks by means of backscatter devices (BD) that may function in constrained spectrums as well as the stringent energy scenarios of green Internet-of-things (IoT) by means of the proposed novel modified backscatter communication model (BCM). Unlicensed eavesdroppers may interfere with the BD due to its vulnerability caused by the wireless communication channels and their broadcasting nature. The intrusion of an unlicensed eavesdropper is detected in an efficient manner by means of the proposed BCM. The analytical derivations of intercept probability (IP) and outage probability (OP) are invoked to analyze the security and reliability of the proposed architecture. Under high main-to-eavesdropper ratio (MER) regime, the IP and under high signal-to-noise ratio (SNR) regime, the OP asymptotic behaviors are estimated additionally. Based on the results of performance evaluation, it is evident that there is a decrease in the security of BD with the increase in MER while there is a simultaneous increase in the legitimate user security. Various system parameters may be adjusted for optimizing the security and reliability performance trade-off. For diverse orders, the existence of error floors are indicated by the non-zero fixed constant of BD and the legitimate user's OP when high SNR value is observed at the system.

Keywords: Intercept probability, Outage probability, Internet of Things, Wireless communication network, Backscatter devices

ISSN: 2582-3167
Submitted: 27.04.2021
Revised: 15.05.2021
Accepted: 1.06.2021
Published: 7.06.2021

1. Introduction

The mobile communication networks of fifth and sixth generation (5G and 6G) face significant challenges in deploying the green Internet-of-thing (IoT) devices that are connected on a massive scale [1]. In order to mitigate global warming, the energy consumption parameters are imposed with several constraints thereby increasing the challenges in this regard [2]. A novel backscatter communication model (BCM) is proposed as the wireless low-power backscatter devices (BD) may be connected in a large scale while enabling efficient communication while supporting green IoT [3]. TV signals, broadcast, Wi-Fi, cellular and other ambient radio frequency (RF) signals may enable energy harvesting as well as data transmission using the proposed modified BCM model when compared to the conventional backscatter models [4]. The high power sinusoidal carrier signals may be eliminated while the signals are modulated and reflected to the BC by the readers in the BCM [5]. The major benefits of BCM technology includes improved spectrum efficiency, low cost, easy deployment and battery free operation. The industry and academia has been extensively performing research in BCM due to its considerable benefits [6, 7].

Several challenges are faced by the conventional BCM technology. Eavesdropping and other security attacks affect the ambient backscatter communications due to the simple modulation schemes and coding. Separation of ambient signals and backscattered signals is also a prominent challenge [8]. The BCM networks and their secure performance is investigated due to its significant applications [9]. Data recovery from RF and BD sources may be performed by the reader by means of the cooperative communication feature of BCM [10]. Various aspects of BCM networks are also investigated by several researchers as observed from the literature. When the presence of an eavesdropper is detected, the legitimate user is notified by the BD and secondary transmitter by transmission and reflection of signals. In the modified BCM network presented, the secondary user physical layer security (PLS) is analyzed. The wireless fading channels and their intrinsic random characteristics may be employed to obtain the PLS [11].

The eavesdropper, BD and legitimate users IP and OP analytical expressions are derived for performing the security and reliability analysis of the modified BCM network [12]. The system parameters are modified to balance between the tradeoff among security and reliability. The

Submitted: 27.04.2021
Revised: 15.05.2021
Accepted: 1.06.2021
Published: 7.06.2021

secondary user's maximum transmitter power and the primary user's peak interference powers are inversely proportional to OP and directly proportional to OP according to the derivations. In systems with high MER and SNR, the eavesdropper, BD and legitimate user IP and OP are estimated via asymptotic analysis [13]. The BD as well as the legitimate user diversity orders are analyzed. A non-zero fixed constant is reached by the BD and the legitimate user OP when the SNR regime is high according to the observations from the work [14]. Zero diversity order and error floor is observed at the OP due to the aforementioned properties. The security of the BD decreases and that of the legitimate user increases with high MER regimes.

2. Related Works

Communication among the secondary transmitters and receivers is established by incorporating the cognitive radio (CR) technology along with the BCM to improve the overall performance of the system. The CR-BCM networks primary and secondary users achievable rates and coverage probability may be estimated with the help of stochastic geometry [15]. The time resources are bit for buyers who are secondary users in the CR-BCM network using auction-based time scheduling techniques. The backscatter symbol detection and a joint channel state information (CSI) feature learning technique are proposed for handling the co-channel direct link interference that causes severe error flow in the conventional energy detector [16]. Between the BCM mode and harvest-then-transmit mode, the time resource allocation is optimized. Energy harvesting and communication modes are considered in the BCM system for maximization of system throughput to overcome the adaptive mode selection issue using reinforcement learning approach [17]. The wireless propagation environments and their broadcasting nature requires large scale connectivity for applications involving future vehicular networks and fifth (5G) generation mobile communication in which secure data transmission is a serious challenge [18]. The wireless fading channels and their intrinsic random characteristics are employed on the basis of an information-theoretic perspective using a physical layer security (PLS) to overcome the aforementioned problem.

The PLS has attracted the interest of various industry and academic researchers over the recent years. When one or more eavesdroppers are present, the multiple cooperative relay utilization for secure source-destination pair communication is studied. The Wyner's Wiretap channel framework is used for establishing secure communications with multiple antennas [19]. The

ISSN: 2582-3167
Submitted: 27.04.2021
Revised: 15.05.2021
Accepted: 1.06.2021
Published: 7.06.2021

communication entities are enabled with secure sessions using symmetric encryption for developing a client-server interaction model based on mutual authentication scheme. In CR networks, the device-to-device communication using PLS is explored by implementing a signal power transmission model [14]. An optimal selection scheme for transmit antenna is proposed a solution for imperfect channel knowledge in multi-antenna cooperative networks for security and reliability solutions in transceivers with hardware impairments by deriving the IP and OP expressions from the theoretical analysis [20]. Individual analysis of the CR and BCM networks is performed for further analysis. The CR and BCM co-existence is to be studied for security and performance optimization in the network.

3. Proposed Work

Figure 1 illustrates the proposed modified BCM architecture in which the eavesdropper, BD, primary user and secondary transmitter modelled. Certain basic assumptions are made in this model such as following independent Rayleigh fading at all channels and equipping single antenna at all nodes. At the secondary transmitter (ST), certain threshold value limits the transmit power (P_T) in order to maintain an optimal quality of communication in the modified BCM network.

$$\mathrm{P_T} = \min\left(P_{max}, \frac{P_{IP}}{|h_{sp}|^2}\right) \text{-------} \ (1)$$

Where h_{sp} is a channel with Rayleigh fading, P_{max} is the maximum transmit power and P_{IP} is the peak interference power at the secondary transmitter.

ISSN: 2582-3167
Submitted: 27.04.2021
Revised: 15.05.2021
Accepted: 1.06.2021
Published: 7.06.2021

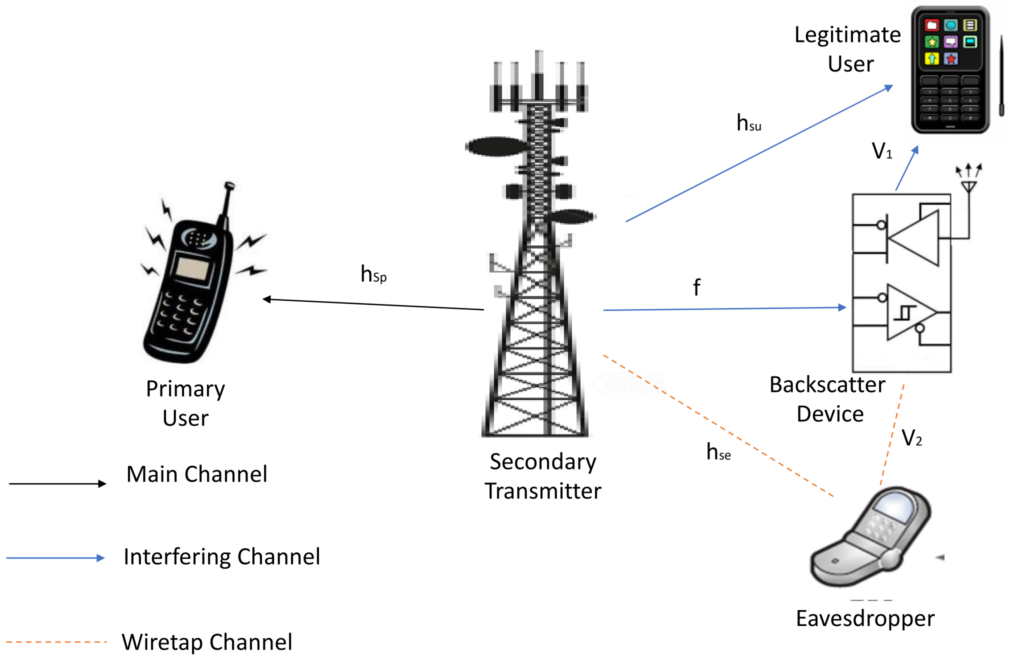

Fig. 1. Proposed Modified BCM Architecture

Further, the signals received at the legitimate user end and that wiretapped at the eavesdropper end are modeled mathematically. The legitimate user receives a signal consisting of the BD based reflecting signal and ST based direct signal. This signal is represented as

$$S_{lu}(t)=h_{su}\sqrt{P_s}x(t)+ \alpha f\beta_1 x(t)m(t)+gn_1(t) \text{ ------(2)}$$

Where m(t) is the ST signal reflected by BD to the legitimate user, α represents the corresponding reflection coefficient, gn_1 is the Gaussian noise and f denotes the probability density function. The signal m(t) is decoded using SIC scheme after decoding x(t) at the legitimate user end. At the eavesdropper end, the wiretapped signal received can be represented using the following expression

$$S_e(t)= h_{se}\sqrt{P_s}x(t)+ \alpha f\beta_2 x(t)m(t)+gn_2(t) \text{ ------(3)}$$

ISSN: 2582-3167
Submitted: 27.04.2021
Revised: 15.05.2021
Accepted: 1.06.2021
Published: 7.06.2021

The BD based backscatter signal and ST based signal x(t) are contained in the eavesdropping signal. gn_2 represents the eavesdropper end complex Gaussian noise signal. The IP and OP are analyzed considering the outage probability and intercept probability. Further, the probability dense function (PDF), cumulative distribution function (CDF) signal-to-interference-plus-noise ratio (SINR) and SNR are estimated. For the legitimate user, the SINR value based on the successive interference cancellation (SIC) technique is given by the following expression

$$R_u = \frac{\lambda|h_{su}|^2}{\lambda|\propto|^2|f|^2|\beta_1|^2+1'} \text{ ------- (4)}$$

At ST, the transmit SNR value is given by $\lambda = \frac{P_S}{\sigma^2}$ where σ^2 is the variance of the complex Gaussian random variable and

$$P_s = min\left(P_{Tmax}, \frac{P_I}{|h_{sp}|^2}\right) \text{ -------- (5)}$$

Where P_{max} is the STs maximum transmit power and the Pus peak interference power is represented as P_I.

4. Results and Discussion

Monte Carlo simulation is used for deriving and verifying the accuracy of the numerical results. Random variables of fading channels are generated using the Monte Carlo trials. Based on the simulation results, it is evident that the analytical results are matched across P_I. Certain errors occur when Gaussian-Chebyshev approximation is used multiple times at high P_I leading to minor discrepancy.

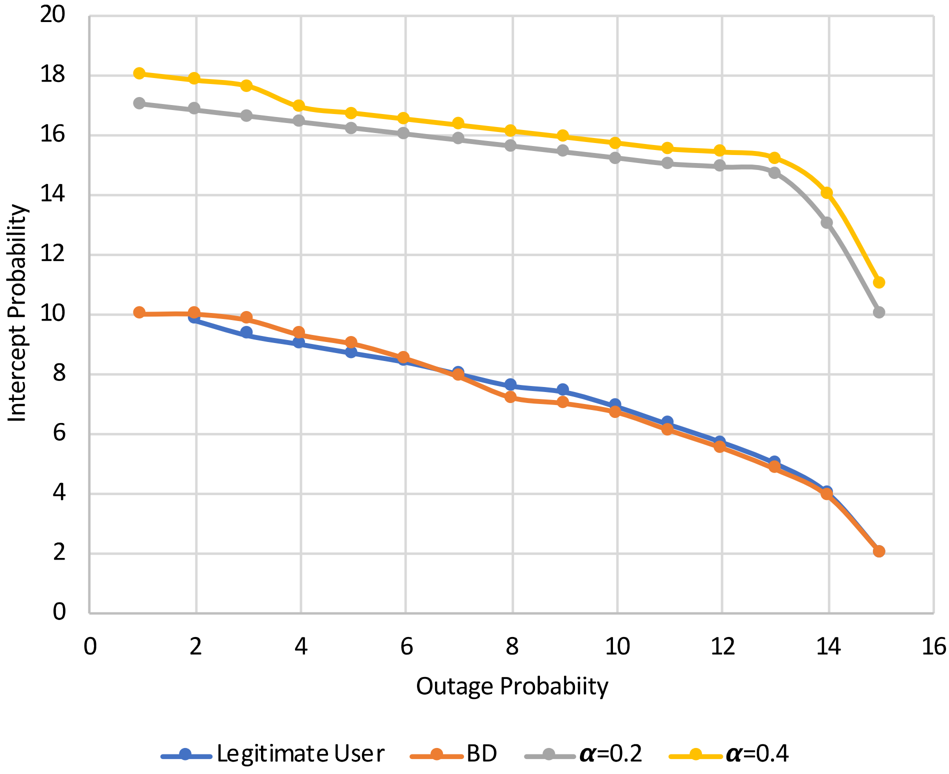

Fig. 2. Intercept and outage probabilities for various trials

Zero order diversity is obtained when a fixed constant is reached by the OP when high SNR and P_I regions are observed. The system security is improved when IP decreases at low P_I regions. The threshold value at the legitimate user end and BD decreases , the IP increases and OP decreases correspondingly leasing to a security-reliability tradeoff. Figure 2 represents the IP and OP values obtained with simulation under various reflection parameters. The probability of the legitimate user information being eavesdropped is reduced significantly by reducing the IP when compared to BD during non-zero constant OP. BD also reflects poor performance while reflecting the information security. Figure 3 represents multiple α values and its corresponding IP and OP values. With the increase in OP of the legitimate user, there is a corresponding increase in α. This improves the user security but negatively impacts the security of α.

ISSN: 2582-3167
Submitted: 27.04.2021
Revised: 15.05.2021
Accepted: 1.06.2021
Published: 7.06.2021

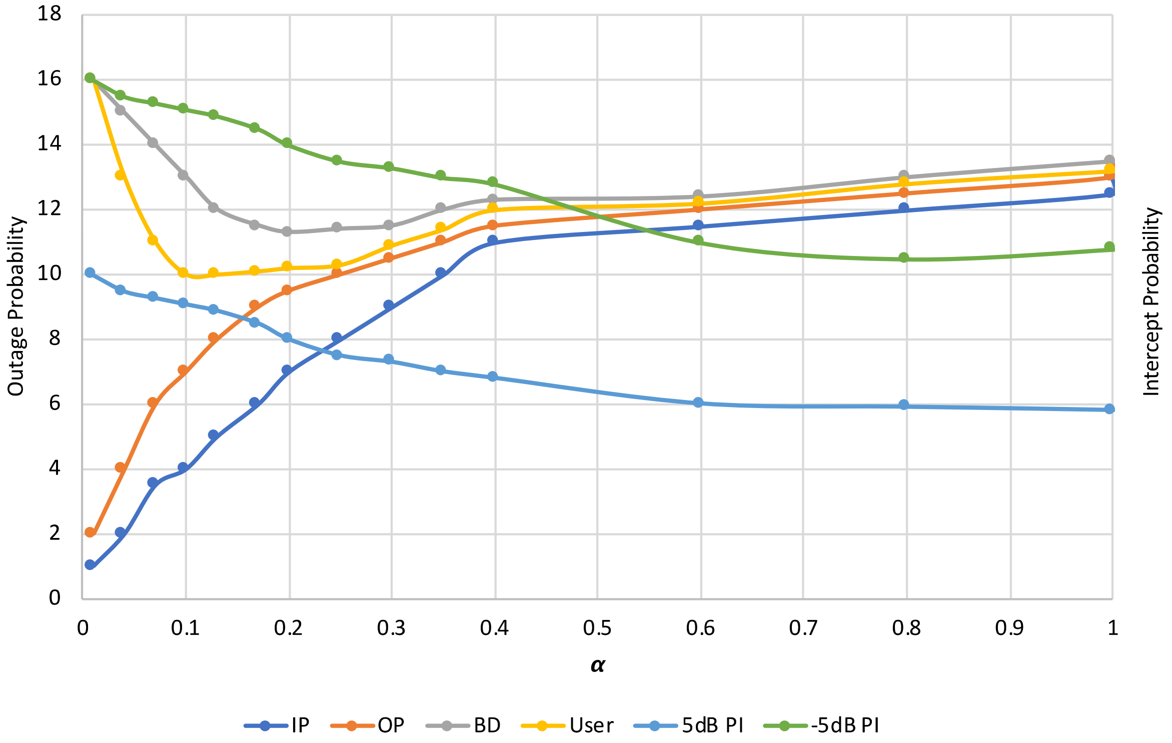

Fig. 3. Intercept and outage probabilities for various α values

Figure 4 represents the intercept versus main-to-eavesdropper ratio under various conditions. The theoretical and asymptotic values of IP are strictly matching in the high MER region. The system security performance is affected in a negative manner when there is an increase in IP caused by the increase in P_I. As MER increases, BD decreases and user security increases irrespective of the P_I value. Under high MER and SNR regimes, the eavesdropper, BD and legitimate user's IP and OP are estimated using asymptotic analysis. Zero diversity orders and error floors are observed in the reflected OP when a non-zero fixed constant is reached by the BD and legitimate user OP under high SNR conditions. The user fails to decode the message of the BD m(t) despite successful decoding of x(t) when an outage event is observed using the SIC technique.

ISSN: 2582-3167
Submitted: 27.04.2021
Revised: 15.05.2021
Accepted: 1.06.2021
Published: 7.06.2021

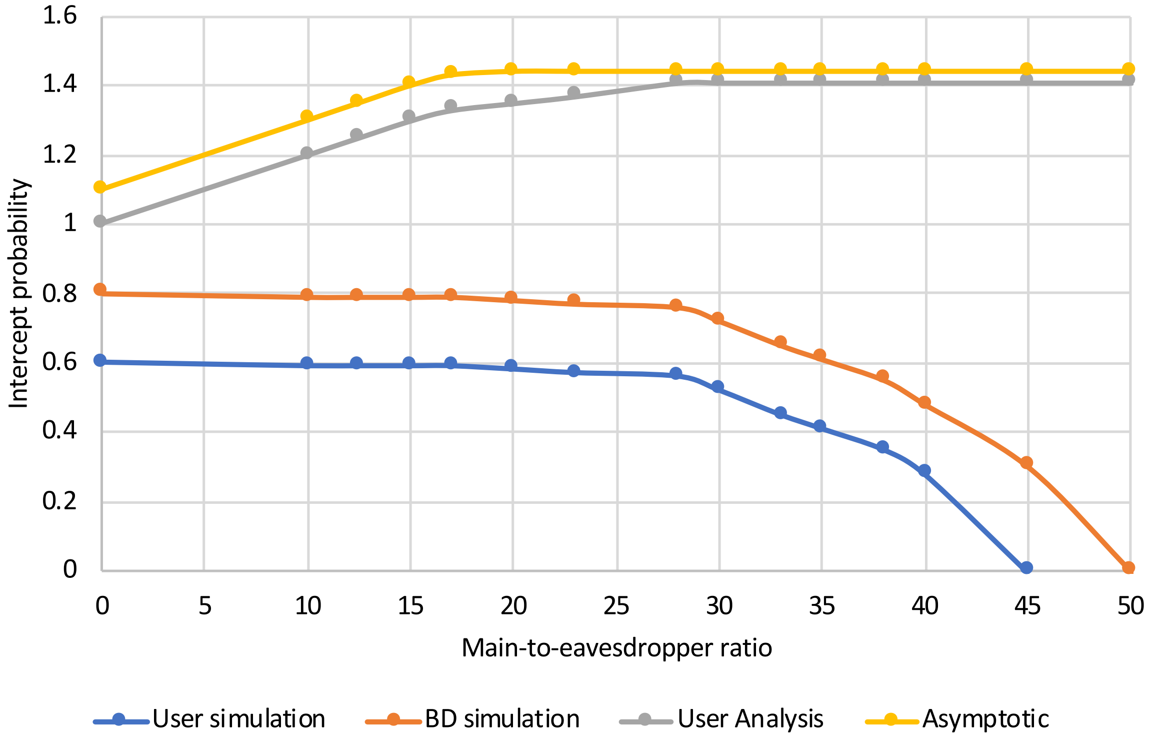

Fig. 4. Intercept versus main-to-eavesdropper ratio

5. Conclusion

The BCM and cognitive radio technology benefits are integrated in the proposed novel BCM architecture. The analytical expressions of IP and OP are derived for the proposed BCM framework and the features are analyzed. In high MER region, the appropriate IP expression and in high SNR region, the asymptotic OP expression are obtained. Considering various system parameters, the security and reliability tradeoff may be adjusted based on the accuracy of the numerical results obtained by the expressions that are derived in this paper. Pmax, PI and SNR threshold values are estimated and their influence on the system performance in terms of reliability and security are analyzed. Future work is directed towards further performance and reliability enhancement.

ISSN: 2582-3167
Submitted: 27.04.2021
Revised: 15.05.2021
Accepted: 1.06.2021
Published: 7.06.2021

References

[1] Ji, B., Chen, Z., Chen, S., Zhou, B., Li, C., & Wen, H. (2020). Joint optimization for ambient backscatter communication system with energy harvesting for IoT. Mechanical Systems and Signal Processing, 135, 106412.

[2] Smys, S., Haoxiang Wang, and Abul Basar. "5G Network Simulation in Smart Cities using Neural Network Algorithm." Journal of Artificial Intelligence 3, no. 01 (2021): 43-52.

[3] Xu, X., Shen, Y., Yang, J., Xu, C., Shen, G., Chen, G., & Ni, Y. (2017, October). Passivevlc: Enabling practical visible light backscatter communication for battery-free iot applications. In Proceedings of the 23rd Annual International Conference on Mobile Computing and Networking (pp. 180-192).

[4] Suma, V., and Wang Haoxiang. "Optimal Key Handover Management for Enhancing Security in Mobile Network." Journal of trends in Computer Science and Smart technology (TCSST) 2, no. 04 (2020): 181-187.

[5] Yang, G., Xu, X., & Liang, Y. C. (2019). Resource allocation in NOMA-enhanced backscatter communication networks for wireless powered IoT. IEEE Wireless Communications Letters, 9(1), 117-120.

[6] Duraipandian, M. "Long Term Evolution-Self Organizing Network for Minimization of Sudden Call Termination in Mobile Radio Access Networks." Journal of trends in Computer Science and Smart technology (TCSST) 2, no. 02 (2020): 89-97.

[7] Zhao, W., Wang, G., Atapattu, S., Tsiftsis, T. A., & Ma, X. (2020). Performance analysis of large intelligent surface aided backscatter communication systems. IEEE Wireless Communications Letters, 9(7), 962-966.

[8] Shrestha, Sujan, and Subarna Shakya. "Technical Analysis of ZigBee Wireless Communication." Journal of trends in Computer Science and Smart technology (TCSST) 2, no. 04 (2020): 197-203.

[9] Liu, W., Huang, K., Zhou, X., & Durrani, S. (2019). Next generation backscatter communication: systems, techniques, and applications. EURASIP Journal on Wireless Communications and Networking, 2019(1), 1-11.

[10] Senthilkumar, M., Kavitha, V. R., Kumar, M. S., Raj, P. A. C., & Shirley, D. R. A. (2021, March). Routing in a Wireless Sensor Network using a Hybrid Algorithm to Improve the Lifetime of the Nodes. In IOP Conference Series: Materials Science and Engineering (Vol. 1084, No. 1, p. 012051). IOP Publishing.

[11] Janeera D.A., Gnanamalar S.S.R., Ramya K.C., Kumar A.G.A. (2021) Internet of Things and Artificial Intelligence-Enabled Secure Autonomous Vehicles for Smart Cities. In: Kathiresh M., Neelaveni R. (eds) Automotive Embedded Systems. EAI/Springer Innovations in Communication and Computing. Springer, Cham.

[12] Kim, T. Y., & Kim, D. I. (2018). Novel Sparse-coded ambient backscatter communication for massive IoT connectivity. Energies, 11(7), 1780.

[13] Xu, C., Yang, L., & Zhang, P. (2018). Practical backscatter communication systems for battery-free Internet of Things: A tutorial and survey of recent research. IEEE Signal Processing Magazine, 35(5), 16-27.

[14] Zeb, S., Abbas, Q., Hassan, S. A., Mahmood, A., & Gidlund, M. (2021). Enhancing Backscatter Communication in IoT Networks with Power-Domain NOMA. In Wireless-Powered Backscatter Communications for Internet of Things (pp. 81-101). Springer, Cham.

[15] Smys, S., & Wang, H. ENHANCED WIRELESS POWER TRANSFER SYSTEM FOR IMPLANTABLE MEDICAL DEVICES.

[16] Raj, J. S. (2019). QoS optimization of energy efficient routing in IoT wireless sensor networks. Journal of ISMAC, 1(01), 12-23.

[17] Sathesh, A. (2019). Optimized multi-objective routing for wireless communication with load balancing. Journal of trends in Computer Science and Smart technology (TCSST), 1(02), 106-120.

[18] Haoxiang, W., & Smys, S. (2020). Soft Computing Strategies for Optimized Route Selection in Wireless Sensor Network. Journal of Soft Computing Paradigm (JSCP), 2(01), 1-12.

[19] Mugunthan, S. R. (2020). Novel Cluster Rotating and Routing Strategy for software defined Wireless Sensor Networks. Journal of ISMAC, 2(02), 140-146.

[20] Dhaya, R., & Kanthavel, R. (2020). A Wireless Collision Detection on Transmission Poles through IoT Technology. Journal of trends in Computer Science and Smart technology (TCSST), 2(03), 165-172.

ISSN: 2582-3167
Submitted: 27.04.2021
Revised: 15.05.2021
Accepted: 1.06.2021
Published: 7.06.2021