Secure Cognitive Wireless Powered Communication Network for Energy Harvesting and Attack Classification

P. Arunachalam[1], Jeyakanth Krishnan[2], Vanitha Soman[3], Dhivya Udhayasuriyan[4]

Department of Biomedical Engineering, Vel Tech Rangarajan Dr. Sagunthala R&D Institute of Science and Technology,Avadi, Chennai, India[1]

Department of ECE, Mangayarkarasi College of Engineering, Paravai, Madurai, India[2]

Department of Electronics and Telecommunication Engineering,Terna Engineering College,Nerul, Navi Mumbai.India[3]

Department of ECE, KLN College of Engineering,Sivagangai, India[4]

Corresponding author: Jeyakanth Krishnan, Email: jeyakanthkrishnan@gmail.com

Construct a cognitive wireless powered communication network (CWPCN) in order to connect with the primary network that is susceptible to eavesdropper (EAVs) protection assaults. A novel cooperative protocol that facilitates collaboration between main users (PU) and secondary users (SU) is proposed here. The SU first extracts energy from the cognitive hybrid access point power signal during the wireless control (WCP) phase, and then uses the captured energy to interfere with EAVs while simultaneously acquiring transmission possibilities during the wireless knowledge transfer phase (within wireless transfers). In accordance with the PU secrecy restriction, the maximization of the SU ergodic rates, resource allotments based on the dual technique of optimisation, and the Block Synchronization technique of Downward Perfect Channel State Information (BSDPCSI). More PU beneficial greedy algorithms to reduce the chance of PU confidentiality are also suggested. Injecting pilot signals and Denial of Service (DoS), Eavesdropping, and Phishing Attacks as jamming to an aggressive intruder will behave in a man-in-the-middle manner. First of all, the channel state information can be identified, and the type of attack can be classified by using the intruder detecting neural net classifier.

Keywords: CWPCN network, eavesdropper, primary users, secondary users, Block Synchronization Method of Downward Perfect Channel State Information, wireless control phase, Channel State Information, intruder detecting neural net classifier

2023. In Satyasai Jagannath Nanda & Rajendra Prasad Yadav (eds.), *Data Science and Intelligent Computing Techniques*, 287–300. Computing & Intelligent Systems, SCRS, India. https://doi.org/10.56155/978-81-955020-2-8-25

1. Introduction

The widespread use of wireless devices has contributed to a rise in interest in complementary technologies. Users have benefited greatly from the development of wireless communications systems, however since wireless signal services are widely dispersed, the contact networks themselves are vulnerable to hostile attacks. In spite of the fact that enhanced mobility protection for wireless networking systems doesn't operate with older wireless networking systems, it did close a major security flaw that affected everything from the physical layer to the device layer. Users need security measures to prevent malicious parties from intercepting their wireless signal. Today's wireless communications networks utilize a variety of encryption methods to circumvent the security issues that arise at the network's highest echelons. Encryption, the process of encoding a message with a secret key generated by a cypher (also known as an encryption technique), is required prior to transmission. If the sender and recipient both have the same key, the message can be deciphered. Higher-level protection can be achieved with encryption, but adversaries on the channel will still be able to pick up on the signal.

Certain applications, such as networks that rely on wireless sensors, may not be able to make advantage of encryption due to the additional complexity and increased power consumption it imposes on the authentication infrastructure. Data security in the wireless domain has to be strengthened so that it can adapt to the new wireless networking architecture. This is why physical layer deployment considerations for communication security have recently developed. Figure 1 shows that the current threats to one's physical safety may be sorted into three classes: jamming, eavesdropping, and spoofing. Physical defence research sometimes uses fictitious characters named Alice, Bob, and Eve to stand in for a valid sender, a legitimate recipient, and a passive invader. Depending on the circumstances, the perpetrator of the assault might be called a jammer or a spoofer.

(1) **Eavesdropping:** Any recipient will receive the message when Alice sends a message to Bob, as the message is transmitted through the whole world. Eavesdropping is a scenario where the message sent by Alice may be received by Eve. The message must be shielded from the wafers.
(2) **Jamming:** A jammer passes the noise type signal to Bob's person to corrupt messages, while Alice and Bob communicate with each other. If Bob receives both signals concurrently, it will receive a valid signal as an unimportant signal. This will not decipher the signal. The assault is called jamming. When the attack happens, legitimate users must recognize it, and the signal must accordingly be secured.
(3) **Spoofing:** Spoofing is a case in which Bob is fooled by the intruder. Double-flow spoofing may be done. (If Alice avoids sending the signal, a deceptive signal is transmitted to Bob by an intruder. (b) Suppose the attacker transmits a signal with a power greater than that of Alice. In that case, Bob will be given a signal from the attacker as a valid signal when finding Alice's signal a signal of interference. This attack must be detected, and appropriate measures are taken, equivalent to jamming.

Although current efforts meet users' safety needs under some circumstances and for particular wireless communication systems, other efforts can fail. Both these drawbacks of current implementations reflect the need for more robust solutions in the physical layer to investigate security risks. Also, energy harvesting (EH) in Cognitive networks is a promising solution for Solving the issue of inefficient use of the spectrum for wireless networking success. In this paper, we suggest a CWPCN concept, offering flexible security strategies for communication systems through the various usage of wireless control security. Protection is given in the current effort when the legitimate receiver is targeted (s). However, before the attack, the security is carried out in the CWPCN definition. In other words, it suggests, in the circumstances outlined in detail in the following pages, that appropriate steps should be taken before the attack takes place. The systems will then change propagation parameters against external threats. The key contributions of the mechanism proposed are,

- The efficiency of wireless networking networks can be increased.
- Reduce the difficulty of the method
- Minimize the rate of data
- Limit the use of energy

2. Related Works

[1] The inefficiency flaw in the original neural network chaotic encryption technique has been corrected in this section. It is suggested to use a neural network chaotic algorithm for wireless secure communication using sophisticated key encryption and decryption. Password-based key exchange systems verify the reliability of a conversation partner by asking for a memorable password. In [2], a brand-new proposal for a wireless 3PAKE is made. The proposed plan is proven correct by the prover if. The effectiveness and safety of the backup system have been improved thanks to the examination of its performance and security. [3] Introduce a novel protocol for using Nave Bayes IDS algorithms in security systems. In order to monitor the whole network for suspicious activity, IDSs are dispersed as multiple agents. Sensors gather data about the agents. The data is extracted, and then processed further. Information from rogue nodes may deter attacks by alerting connected IoT items or the administrator. In addition, IDS-based solutions are more practical for the IoT setting because of lower installation and ongoing maintenance expenses. To enhance network security in restricted WSNs, [4] suggests activating trustworthy neighbors depending on their functions. The two stages of AF-TNS's operation are confidence assessment for energy constraints and confidence assessment for metric nodes. The dynamic decision-making process of the AF is simplified by the random Tran sigmoid feature, which distinguishes between reliable and suspect network outcomes. Results from computer simulations show that AF-TNS improves network efficiency by increasing identification rate and preserving network lifetime. [5]. An ultra-light RFID (ULRMAPC) protocol protection scheme is presented. They reasoned that with some work, their protocol might be used to provide robust security for IoT infrastructure. However, they show in this work that their protocol is susceptible to DoS attacks, reader and tag impersonation, and synchronization. To get around this problem, they suggest a new reliable authentication mechanism that may be utilized with RFID-based IoT devices.

[6] In this research, the authors examine the proposed outgoing protection systems and address the challenges of cyber sensing tactics for protecting AVNs. In addition, an SFA (Aircraft Protection Framework) is suggested as a safeguard against attacks on aircraft structures by physical touch. According to the numerical results, SFA has a far higher detection and prediction rate than the currently used intrusion detection for an aero plane communication system. [7] Software that uses signal intensity instead of external devices like GPS or antennas or air monitors or centralized authorities like certification authorities is proposed. When malicious identities are detected, the mobile nodes isolate and blacklist them to prevent any further data exchange with them. Using an analysis of the signal strength received by each node, the proposed attack tracker may identify the presence of Sybil attacks and locally repeated assaults. They also propose a way to counteract these assaults throughout the whole network. We put our theories to the test by simulating them in NS-2 and putting them to the test on a global scale. The results demonstrate that sophisticated gear, periodic photos, or a pricey location are not required to witness identity assaults in ad hoc wireless networks with a high degree of accuracy. [8] To maximize the possible eavesdropping intensity within the transmitting power limitation at the legitimate control and the interruption temperature limit at the main receiver, this was envisioned as a non-convex problem with infinite bounds. Second, by imposing bounded constraints on the original issue, it is become tractable. An empirical solution of relatively low complexity is then presented for the streamlined issue. Finally, numerical data are presented to evaluate our suggested solutions for UAV-enabled wireless networking. [9] This article presents the Hamming Residue System (HRM), a method for reducing the impact of cyberattacks. Results from the tests validate the recommended approach. [10] An algorithm for encrypting and decrypting hybrid WSN data has been developed. AES, a symmetric key method, is used for both the encryption and

decryption processes. Since these two methods can both benefit from our new approach, we have developed it. Since the key exchange issue in AES has been resolved, the suggested technique is simpler than AES and reduces complexity in comparison to ECC; nonetheless, it is only utilized for key generation and not data encryption.

[11] It proposed a number of different configurations of modulation schemes with varying degrees of spectrum performance, energy economy, and security. The scheme also incorporates signal mixing between a large pool of possible subcontractors, giving the eavesdropper tens of thousands of options to fool. In terms of bit errors, the simulation results imply that the proposed modulation of square amplitude is the most effective. [12]. The goal of this study is to compare the impact of security and efficiency in contemporary lightweight block cypher systems on the requirements of resource-constrained industrial wireless sensor networks. Then, the results of various cryptosystems were assessed on a computer using a variety of measures, including memory occupancy, byte cycles, throughput, and others. It also presents the avalanche effect, which shows how likely it is to withstand various types of assaults. According to their findings, SPECK is the most effective lightweight software-based chipboard in terms of protection and performance across a variety of metrics. [13] The approach proposed for security risk assessment improved upon the evaluation procedure established by the GMITS model (ISO13335). The findings of an asset analysis, threat/vulnerability analysis, and opportunity analysis were used by the protective risk management system to finally quantify risk and define danger rating. Key issues encountered by smart automobiles are targeted increases in vehicle speeds and breaches of personal data; the recommended approach was applied to examine these concerns. The system was expanded to include the new threats of increased velocity and the disclosure of sensitive information. [14] repair MQTT flaws that snoopers might employ to spy on unprotected networks. This work presents a lightweight and fuzzy logic detection approach called Secure-MQTT for detecting malicious behavior during IoT communication between devices. The proposed method employs a flurry-based logic methodology to identify malicious behavior's by the node. With the help of the dynamic rules generation interpolation, Secure-MQTT is able to avoid the need for a large rule base. The proposed method provides a useful tactic for shielding low-configuration PCs against DDoS assaults. The results of the simulations show that the suggested strategy can more accurately forecast assaults than existing methods. [15] addresses the issue of delay caused by a decision-making system for band selection, which has serious consequences for both security and efficiency. Based on the idea of clusters, a new paradigm for cooperative spectrum sensing is developed. In this setup, CHs are swapped with other CHs and shared nodes for the sake of monitoring. This paradigm significantly shortens the time it takes to perform tasks like sensing, integrating, routing, and selecting a band. This also reduces the amount of power needed for spectrum detection, which is a major factor in the overall efficiency.

3. Problem Statement

Three of the most important risks to wireless communication are:

- **Denial of service attacks** - if the intruders inundate the network with messages affecting the network services available
- **spoofing and hijacking of the session** - when the intruder achieves access by taking the identity of a valid person to the data and services of the net
- **the removal of information** - where unauthorized third parties intercept data sent by a protected network

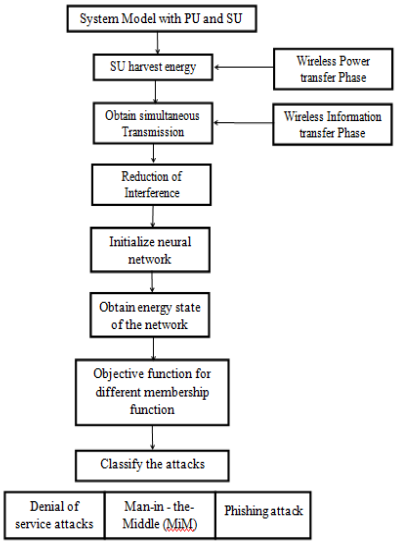
Users should make every attempt to correctly configure the wireless network communication device to address these risks.

4. Proposed Methodology

The general logic of the suggested process is shown below. Here is the intended overall flow,

a. System model

The condition has been studied for two groups of incorporated users, namely SUs and PUs. For example, PUs, handsets, wireless micros, or televisions make a wireless spectrum. On the other hand, SUs are suggested for those without a new wireless spectrum. Equipped SUs with cognitive radios should instead submit their individual packets by shielding them if they do not use the approved wireless spectrum. The free wireless spectrum is further split into various networks of the same frequency bandwidth from PUs. When all other nodes are sustainably powered, the SU will accumulate RF resources. Our job can be used to avoid the mutual interruptions in the multi-SU case, in which multiple SUs can transmit data orthogonally, e.g., by dividing time or frequency. In any slot or frequency band, our scheme is applicable when one entity consumes energy or transmits data.



b. Wireless power and information transfer phase

This sort of set up may initially be done in order to analyze the activities of both the primary user (PU) and the secondary user (secondary user) and to eliminate interference. The PU that was chosen in step 1 is going to be referred to as PU_a. from here on. In tandem with PB's wireless power transfer to PU, SUa's transmission of data to a secondary receiver makes use of the maximum power available, denoted by $\hat{q}_s$.The energy harvesting (EH) phase will begin only if the received signal is stronger than the sensitivity. The SU is able to extract energy from the PU_aas well as the power source. This energy may be represented as

$$\varepsilon_q = \eta\tau\left(q_e G_{qe} \ell_{qe} + \hat{q}_s G_{bq} \ell_{bq} - \gamma_{th}\right)^+ \quad (1)$$

No energy harvesting will occur in Phase II if the EH-phase of SU is not enabled in Phase I. If SU has collected energy during Phase I, it will use that energy to power its data transmission to the access point during Phase II. The SU transmit power, denoted by the symbol Qq, is

$$Qq = \frac{\mathcal{E}q}{1-\tau} \tag{2}$$

The likelihood that the power of SU may be approximately represented by a given discrete power can be computed based on the best PU selection made in Phase I.

$$qr\{Q_q \approx Q_{q_n}\} = \frac{\hat{q}_s}{q_e \ell_{qe}}\left[h\left(\frac{(1-\tau)L_{n+1}}{\eta\tau\hat{q}_s} + \frac{\gamma_{th}}{\hat{q}_s}\right) - h\left(\frac{(1-\tau)L_n}{\eta\tau\hat{p}_s} + \frac{\gamma_{th}}{\hat{p}_s}\right)\right] \tag{3}$$

The equation (3) can be rewritten as,

$$h(\gamma) = \left(\frac{\hat{q}_s}{q_e \ell_{qe}}\right)^{-1}\left[1 - \exp\left(-\frac{\hat{q}_s\gamma}{q_e \ell_{qe}}\right)\right] + (-1)^1 \sum_{(i_1)\epsilon\upsilon\kappa,1}\left(\frac{\hat{q}_s\gamma}{q_e \ell_{qe}} - \frac{1}{\ell_{i_1 q}}\right)^{-1}\left[\exp\left(-\frac{\gamma}{\ell_{i_1 q}}\right) - \exp\left(-\frac{\hat{q}_s\gamma}{q_e \ell_{qe}}\right)\right] + \ldots + (-1^K) \sum_{(i_1 \ldots, i_k)\epsilon\upsilon\kappa,k}\left(\frac{\hat{q}_s\gamma}{q_e \ell_{qe}} - \frac{1}{\ell_{i_1 q}} - \cdots - \frac{1}{\ell_{i_k q}}\right)^{-1}\left\{\exp\left[-\left(\frac{1}{\ell_{i_1 q}} + \cdots + \frac{1}{\ell_{i_k q}}\right)\gamma\right] - \exp\left(-\frac{\hat{q}_s\gamma}{q_e \ell_{qe}}\right)\right\} \tag{4}$$

Here the interference-assisted energy harvesting can be done, and the allocations of resources can be done using the dual optimization approach and the Downward Perfect Channel State Information Block Synchronization Method. The protection of the block synchronization technique shows the importance of maintaining data source validity. Specific techniques are integrated into such synchronization protocols to tackle false time stapes or to prevent malicious attacks.

Initially, by establishing the limit/range for the channel state information, the user positions utilized in the network may be formed. The range is then divided up between the users and their respective base stations. If, for instance, it has been decided that the maximum number of users in a certain area is 100, all the users inside that area will be grouped together and connected to the same base station. The suggested approach divides the recognition position into three stages. The node's location is first linked to the use of the Euclidean distance measure. Then, the forecasts of the user to the side are used. The next step is to determine the principal user's coverage parameters and then compute the temporal relationship between the two nodes. Third, we anticipate typical non-active channels. After then, data from the channel is sent to the cluster head so that a confidence level in idle sensing may be determined. In the end, the remaining energy is updated to reflect the state of the energy used by the routing and communications systems.

c. Correlation and confidence based neighbor user selection:

A WCN may be dormant until an event occurs, at which point a routing mechanism for the transfer of the sensed data is designed and implemented. Since the nodes' values correlate when they detect a nearby event, the sensed data retains its spatial consistency. Values that are statistically similar to those near nodes are identified. However, proximity (measured in terms of the Euclidean distance between nodes) might vary widely depending on case details and design considerations. Any of the applications could not be more important, and the detected values differ in a pragmatic event, necessitating closer data presentation at the node level (where correlation is less). It's possible that some other program provides a more accurate representation of detected values, but neighbors aren't required to share their information. Utilizing spatial correlation for controlling the number of nodes that gather redundant information helps save power, which is crucial to the continued viability of any given network.

$\delta=\sqrt{\vartheta(1,\gamma_1)-\vartheta(1,\varphi_1)^2+\vartheta(2,\gamma_1)-\vartheta(2,\varphi_1)^2}$

Estimate spatial correlation,

$\tau=\min(x,y)$ (5)

Node $\epsilon_{node}=1-(\delta(x,y)/\tau)$ (6)

d. Temporal correlation among two nodes:

It may be possible to connect data from the same sensor obtained at various periods. The relationship between time and this is also defined. Because of the nature of the physical world, the most important aspect of each new sensor node analysis has been temporal, with the cumulative findings often being comparable only within a constrained time window. Sensor nodes have no intention of broadcasting their reading until the current analysis is under an acceptable threshold error in terms of the length reading. The sink node will infer any missing information from the usual data sources. Correlation between successive sensor readings might change at different rates depending on the nature of the phenomena. The next step would be to use the well-known idle channel prediction. Measurements of detecting idle channel confidence are then relayed to the cluster head, following which the rest energy is adjusted.

To determine the cumulative distribution function, one may use the formula

$$F_z(z)=\mathrm{qr}\left\{\max_{i\epsilon\mathcal{K}} G_{iq}\ell_{iq}\le z\right\}=$$
$$\prod_{i=1}^{k}\left[1-\exp\left(-\frac{z}{\ell_{iq}}\right)\right]=1+(-1)^1\sum_{(i_1)\epsilon\upsilon_{K,1}}\exp\left(-\frac{z}{\ell_{iq}}\right)+\cdots+(-1)^k\sum_{(i_1\ldots,i_k)\epsilon\upsilon K,k}\exp\left[\left(-\frac{1}{\ell_{i_1q}}-\cdots-\frac{1}{\ell_{i_kq}}\right)\right]z \quad (7)$$

"The average performance, which may be expressed as, is used to calculate the peak power.,

$$\mathrm{Qr}\{Q_q\approx Q_{q_n}\}=1-\frac{\hat{q}_s}{q_e\ell_{qe}}h\left(\frac{(1-\tau)L_N}{\eta\tau\hat{q}_s}+\frac{\gamma_{th}}{\hat{q}_s}\right) \quad (8)$$

Phase I involves a high-power transmission from the chosen PU to a secondary receiver. After deducting the energy signal from the composite signal, the SR then represents the data signal's maximum attainable rate as,

$$d_{br}=\log_2\left(1+\frac{\hat{q}_sG_{br}\ell_{br}}{v_0}\right) \quad (9)$$

In Phase II, SU will remain quiet if its EH phase was not engaged in Phase I. The PU with the best channel conditions for PR is enabled to broadcast at $\hat{q}_s$. The chosen PU is indicated by the notation PUv, wherev = argmaxi∈Girℓir.. Obtainable rates at SR are calculated as,

$$d_{vr}=\log_2\left(1+\frac{\hat{q}_sG_{vr}\ell_{vr}}{v_0}\right) \quad (10)$$

In Phase II, SU will send data to AP if it has collected enough energy from its harvest in Phase I. Each PU is capable of determining its own legal power output, which is expressed,

$$q_{s_i} = \min\left\{\hat{q}_s, \frac{Q}{G_{ia}\ell_{ia}}\right\} \quad (11)$$

Because of disruptions in the signal, we may express the total quantity of data delivered as,

$$d_{pa} = \log_2\left(1 + \frac{p_p G_{pa}\ell_{pa}}{p_{s_q} G_{qa}\ell_{qa} + v_0}\right) \quad (12)$$

The maximum achievable secondary reception rate for PR in phase II with SU transmission interference is,

$$d_{qr} = \log_2\left(1 + \frac{q_{sq} G_{qr}\ell_{qr}}{q_q G_{qr}\ell_{qr} + v_0}\right) \quad (13)$$

Assuming SU has a constant data transfer rate to AP, we may write this as,

$$d_n = (n - dt)V_{dt1} \quad (14)$$

As more data is obtained, the level of interference will decrease. This will allow the interference to be categorized.

After obtaining channel and energy status data, the neural network may be initialized for attack categorization. First, the neuron must be initialized.

$$a_j^l = \sigma \sum_K W_{jk}^l a_K^l + b_j^l \quad (15)$$

A vectorized version of the equation is possible,

$$a^l = \sigma\left(w^l a^{l-1} + b^l\right) \quad (16)$$

The goal of backpropagation is written in the quadratic form,

$$C = \frac{1}{2N}\sum_X \left|y(X) - A^l(x)\right|^2 \quad (17)$$

The C function can be written in the form of,

$$C = \frac{1}{N}\sum_x C_x \quad (18)$$

The same C function can be written in the quadratic form,

$$C_x = \frac{1}{2}\left\|Y - a^l\right\|^2 \quad (19)$$

The quadratic set in which the training set can be merged,

$$C = \frac{1}{2}\left\|Y - a^l\right\|^2 = \frac{1}{2}\sum_j (y_j - a_j^l)\text{^}2 \quad (20)$$

The energy in the neuron can be represented as,

$$\delta_j^l = \frac{\delta_C}{\delta_{z_j^l}} \tag{21}$$

The objective function for different membership function can be represented in the form of the matrix,

$$\delta^l=(a^l - y) * \sigma^1(z^l) \tag{22}$$

For classifying the attack,

$$\partial^l = ((W^{l+1})^T \partial^{l+1} * \sigma^1(Z^L) \tag{23}$$

The gradient classified output is given by",

$$\frac{\partial C}{\partial w_{kj}^l} = ak^{l-1} \tag{24}$$

The algorithm for this approach is shown below:

Algorithm 1: dual method of optimization and the Block Synchronization Method of Downward Perfect Channel State Information and attack classification

Input: Usernodeinitialization
Output: Attack classification

Step1: *initialize the user*
Communication_radius
Desipation_energy
initial_energy
movement_speed=randi([1 50],length
no_packets=rand([10 20],length
Step2: calculate Euclidean distance estimation
for i=1:length
for j=length
$\delta=\sqrt{\vartheta(1,\gamma_1) - \vartheta(1,\varphi_1)^2+\vartheta(2,\gamma_1) - \vartheta(2,\varphi_1)^2}$
end
Step3:Estimate Spatial Correlation
for xi=1:length
for yi=1:length
spatial_radiusminif
selection_node

end
end
end
step 4: Neighbour Node Prediction
for xi=1:length
neighbor_listfind(sc_node=~0)
end
step 5: channel sensing process

```
    for ii=1:length(idelchannel)
choose_idle=randi([1 30 ],noidelchennal(ii))
  end
step 6: Confidence Level estimation about the estimated idle channel at BS
for cc=1:
 if temp_node==1
confidence_node
end

step 7: attack classification
residula_energy
packet_sent=no_packs*
malicious node classification
end
end
```

5. Result And Discussion

This section depicts the performance evaluation of the suggested method. Table 1 displays the proposed system's simulation parameters.

"**Table 1** simulation parameters of the proposed system"

Parameters	values
Energy transmission	60.0 m
Energy sampling	20 .0
Energy amplitude	0.00123 m
Energy aggregate	5 kWh
Primary user	150
Secondary user	150
Number of packets	Random of 10-12
Square area size	1000*1000 m^2
Velocity	[10,40] m/s

e. Comparative analysis of proposed and existing mechanism in terms of different number of maximum speed

"Below are the findings of an analysis that compared two sets of SUs based on (a) the average end-to-end latency and (b) the mean energy usage per transmission packet in both existing and forecasted methods. Thus the technologies proposed show that the method proposed is better than the other existing strategies such as channel allocation and connection scheduling (SRLC), J-SRCA [16], and IHA [17].

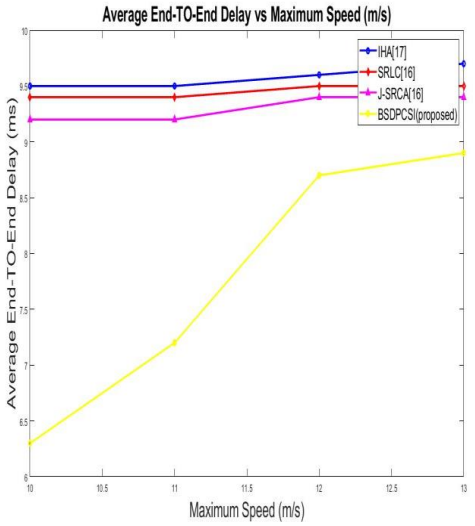


Figure 1 (a) Average end-to-end delay vs. maximum speed

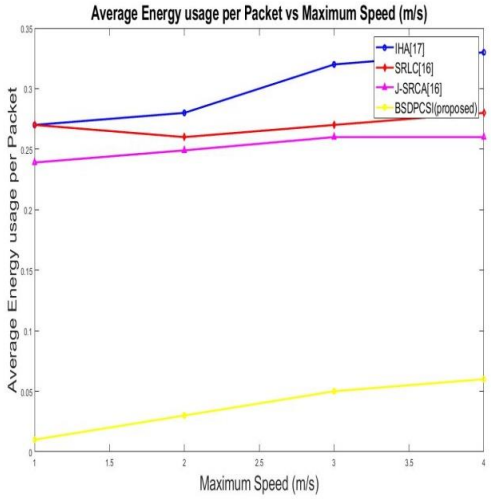


Figure 1 (b) Goodput vs. maximum speed

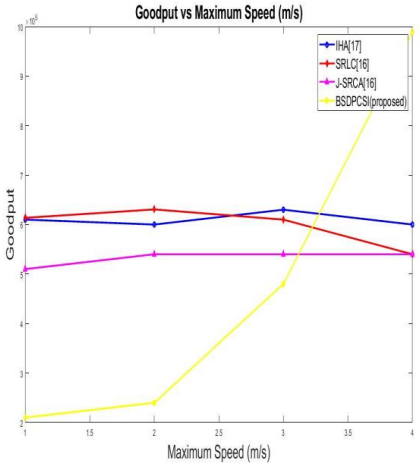


Figure 1(c) Average energy usage vs. maximum speed

Figure 1a indicates an improvement in delay due to the speed of mobility. The higher pace increases the chances of breaking the connection and restoring the excess route. In comparing the predicted system, a time-to-end delay is increased, hence the likelihood of a connection interruption is minimized. As seen in Figure 1a. The positive thing ends in Figure 1b, with the improved agility speed. The exact lifetime estimation of the relation and direct use in an exaggerated way of comparing current methods of this neighborhood selection metric results Figure 1c indicates the energy consumption for packet vs. various high speeds transmission. The protocol suggested would work more effectively than the current mechanism, regardless of the rise in energy demand.

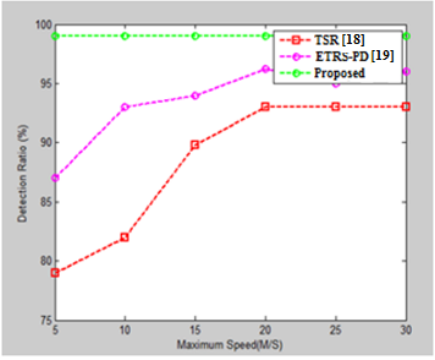


Figure 2 Maximum Speed vs. Detection Ratio (%)

The nodes move rapidly, as depicted in Figure 2. The links between nodes are constantly increasing. This results in higher identification rates for malicious clone nodes. The performance of the suggested classification of neural networks is higher than the performance of the detection ratios of TSR [18] and ETRS-PD[19]. The proposed mechanism has better detection ratios, especially at higher velocity.

Using several types of malicious nodes and attack detection, this second study compares the proposed technique to the current TSR and ETRS-PD methods.

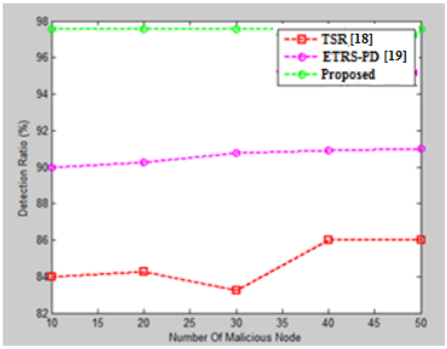


Figure 3 Number of malicious node vs. Detection Ratio

Table 2 comparison between average opportunity discovery and PU channel use.

	Techniques	PU channel utilization										
SNR		0	.1	.2	.3	.4	.5	.6	.7	.8	.9	1
Average opportunity	Cluster CMSS policy discovery [20]	0.970	0.960	0.950	0.930	0.900	0.850	0.770	0.720	0.650	0.60	0.570
	Greedy Non-cooperative policy [20]	0.870	0.860	0.860	0.860	0.850	0.830	0.770	0.730	0.650	0.58	0.510
	Genie aided location aware policy [20]	1	1	1	0.970	0.960	0.940	0.900	0.840	0.790	0.700	0.700
	CWPSN [20]	1	1	1	1	1	1	1	1	1	1	.080
	Proposed system	1	1	1	1	1	1	1	1	1	1	1

The data shown in table 2 illustrate the average opportunity discovery in relation to PU channel utilization. It presents a comprehensive depiction of the outcomes obtained from the suggested approach, specifically focusing on the utilization of the primary user channel. The findings are quantified on a scale ranging from 0 to 1, demonstrating a satisfactory resolution. From the result obtained the suggested methodology outperforms well than other existing system in use.

6. Conclusion

A system model is originally created depicting the user's execution of SU movement and PU duties. Each node in the network has been defined in three different situations. The predicted channel availability from these cases is stored in the Block Synchronization System of Downward Perfect Channel State Information. Finally, with the help of the new classifier, we can identify the reliable node and characterize the assault. The end-to-end latency, in particular, is shown by the simulation results to benefit from the described algorithm's implementation".

References

[1] Liang, C., Zhang, Q., Ma, J., & Li, K. (2019). Research on neural network chaotic encryption algorithm in wireless network security communication. EURASIP Journal on Wireless Communications and Networking, vol.2019,no.1, pp.1-10.

[2] Chen, C. M., Wang, K. H., Yeh, K. H., Xiang, B., & Wu, T. Y. (2019). "Attacks and solutions on a three-party password-based authenticated key exchange protocol for wireless communications". Journal of Ambient Intelligence and Humanized Computing, vol.10,no.1,pp.3133-3142.

[3] A. Mehmood, M. Mukherjee, S. H. Ahmed, H. Song, and K. M. J. T. J. o. S. Malik, "NBC-MAIDS: Naïve Bayesian classification technique in multi-agent system-enriched IDS for securing IoT against DDoS attacks," vol. 74, no. 10, pp. 5156-5170, 2018.

[4] O. AlFarraj, A. AlZubi, A. J. J. o. A. I. Tolba, and H. Computing, "Trust-based neighbor selection using activation function for secure routing in wireless sensor networks," pp. 1-11, 2018.

[5] S. F. Aghili, M. Ashouri-Talouki, and H. J. T. J. o. S. Mala, "DoS, impersonation and de-synchronization attacks against an ultra-lightweight RFID mutual authentication protocol for IoT," vol. 74, no. 1, pp. 509-525, 2018.

[6] H. Sedjelmaci and S. M. J. T. J. o. S. Senouci, "Cyber security methods for aerial vehicle networks: taxonomy, challenges and solution," vol. 74, no. 10, pp. 4928-4944, 2018.

[7] M. Faisal, S. Abbas, H. U. J. E. J. o. W. C. Rahman, and Networking, "Identity attack detection system for 802.11-based ad hoc networks," vol. 2018, no. 1, p. 128, 2018.

[8] Faisal, M., Abbas, S., & Ur Rahman, H. (2018). Identity attack detection system for 802.11-based ad hoc networks. EURASIP Journal on Wireless Communications and Networking, vol.2018, no.1, pp.1-16.

[9] Alotaibi, M. (2019). Security to wireless sensor networks against malicious attacks using Hamming residue method. EURASIP Journal on Wireless Communications and Networking, vol.2019,no.1,pp. 1-7.

[10] S. Prakash and A. Rajput, "Hybrid cryptography for secure data communication in wireless sensor networks," in Ambient Communications and Computer Systems: Springer, 2018, pp. 589-599.

[11] T. Maksymyuk, M. Beshley, M. Klymash, O. Petrenko, and Y. Matsevityi, "Eavesdropping-resilient wireless communication system based on modified OFDM/QAM air interface," in 2018 14th International Conference on Advanced Trends in Radioelecrtronics, Telecommunications and Computer Engineering (TCSET), 2018,no.1, pp. 1127-1130: IEEE.

[12] C. Pei, Y. Xiao, W. Liang, X. J. E. J. o. W. C. Han, and Networking, "Trade-off of security and performance of lightweight block ciphers in Industrial Wireless Sensor Networks," vol. 2018, no. 1, p. 1-17, 2018.

[13] H.-K. Kong, M. K. Hong, T.-S. J. J. o. A. I. Kim, and H. Computing, "Security risk assessment framework for smart car using the attack tree analysis," vol. 9, no. 3, pp. 531-551, 2018.

[14] A. Haripriya, K. J. E. J. o. W. C. Kulothungan, and Networking, "Secure-MQTT: an efficient fuzzy logic-based approach to detect DoS attack in MQTT protocol for internet of things," vol. 2019, no. 1, p. 90-99, 2019.

[15] M. A. Mirza, M. Ahmad, M. A. Habib, N. Mahmood, C. N. Faisal, and U. J. T. J. o. S. Ahmad, "CDCSS: cluster-based distributed cooperative spectrum sensing model against primary user emulation (PUE) cyber attacks," vol. 74, no. 10, pp. 5082-5098, 2018.

[16] S. Amiri-Doomari, G. Mirjalily, and J. Abouei, "Stability-based routing, link scheduling and channel assignment in cognitive radio mobile ad-hoc networks," Wireless Networks, vol. 25, no. 4, pp. 2013-2026, 2019.

[17] T. P. Nghiem, T. H. J. J. o. P. Cho, and D. Computing, "A fuzzy-based interleaved multi-hop authentication scheme in wireless sensor networks," vol. 69, no. 5, pp. 441-450, 2009.

[18] R. Chen, F. Bao, M. Chang, J.-H. J. I. T. o. P. Cho, and D. Systems, "Dynamic trust management for delay tolerant networks and its application to secure routing," vol. 25, no. 5, pp. 1200-1210, 2013.

[19] Ma, B., Sb, S. P., & Rc, A. C. (2021). Fuzzy based clustering in CWPSN using machine learning model. Indian Journal of Radio & Space Physics,vol.50,no.1,pp. 90-94.

[20] R. H. Jhaveri, N. M. Patel, D. C. Jinwala, J. Ortiz, and A. de la Cruz, "A composite trust model for secure routing in mobile ad-hoc networks," in Ad Hoc Networks: InTech, vol.2017, no.1,pp. 19-45.