Spectrum Sensing based Trust Aware Routing for Cognitive Radio Ad hoc Networks (CRAHNs)

Bosupally Nanda Kumar
Ph.D Scholar, Departrment of ECE
Osmania University, Hyderabad, Telangana

K. Jaya Sankar, PhD
Professor, Department of ECE
Methodist College of Engineering and Technology (Autonomous), Abids, Hyderabad, Telangana

ABSTRACT

Routing in Cognitive Radio Ad hoc Networks (CRAHNs) is a regarded as a challenging task due to the dynamic nature of frequency bands in Cognitive Radio technology. Due to varying frequency bands, the traditional networking routing protocols cannot be applied over CRAHNs. Further, the unavailability of channel information also impacts the network performance. Along with these issues, the presence of adversary nodes and their malicious actions deteriorates the network performance drastically. Hence, this paper introduces a new routing mechanism called as Spectrum Sensing based Trust Aware Routing (SSTAR) for CRAHNs. According to SSTAR, each node subjects to the computation of a trust value, cost associated with channel linked and the probability of the presence of Primary users. SSTAR forms a composite metric is formulated and establishes a secure path for source and destination node pair in the network. Simulation experiments on the proposed SSTAR prove the efficiency in terms of packet delivery ratio, delay and malicious detection rate.

General Terms

Wireless Network, Dynamic Spectrum Access, Secure Routing.

Keywords

Cognitive Radio Ad hoc Networks, Security, Trust Value, Spectrum Sensing, Routing.

1. INTRODUCTION

Cognitive Radio Adhoc Networks (CRAHNs) is one of the promising technologies and it acquired much attention towards wireless communication [1]. Usually, CRAHNs has wide range of applications like intellectual convey systems, smart grid communications, civic safety systems, dynamic spectrum admittance, and cooperative networks [2]. The research towards CRAHNs is increasing due to its capability to solve the major issues related to spectrum demand and restricted spectrum supply for the rising wireless applications and its service provisions. There are two major categories of users in the CRAHN; they are Licensed User (LU) or Primary user (PU) and Cognitive User (CU) or Secondary User (SU). Among these two users, LU has authorization to utilize the certain frequency but CU does not have any license to use the specific frequency of radio spectrum. But there is a possibility to use the LU's frequency without creating any interruption to the transmission of LU [3-5].

Spectrum sensing is the process in CRAHN technology to detect the unused frequency bands called as spectrum holes and utilizing them to help in data transmission. Even though spectrum sensing has less accuracy for the detection of spectrum holes, it is more flexible and inexpensive when wide range of network is considered [6]. Spectrum access strategies enable the development of communication algorithms and protocols due to its adaptability and dynamism for the identification and exploitation of spectrum gaps, reduction of interference between communicating nodes, minimization of channel congestion, and the improvisation of average channel efficiency. In the rapid advancement and distribution of CRN, security is found as one of the major challenging constraints due to the coexistence of SUs along with PUs [7-8]. Moreover, spectrum sensing is also considered as major challenging issue when LU is operated with different data rates, modulations, and transmitted power [9].

During spectrum sensing, every CR node is prone to multiple security attacks. The CR technology itself is vulnerable to get attacked when the transmitter transmits a signal at the same frequency with sufficient power can block or jam the radio frequency. In this situation, there is a threaten to the security of LU due to the uncontrollable behavior of CU. Hence, security is considered in order to construct specific routing protocols for CRN in two different approaches [10]. Encrypting the control and data messages exchanged over the various pathways is the first method of protecting the routing algorithm or protocol, which includes protecting the route formation, route maintenance, and data forwarding procedures. The second method is to use security as a routing metric to identify the best nodes and optimal path. In this regard, the proposed work concentrated on security provision during the spectrum sensing to protect the LU from the malicious attacks and to ensure a secured route from the source to destination by considering several metrics like trust value, channel cost, and the probability of presence or absence of LU. Here, the major contributions of the proposed research work are outlined as follows;

1. To monitor the CUs behavior and PUs activity during spectrum sensing stage, this work proposes a trust value based malicious nodes detection mechanism.
2. To enhance the network performance and security, this work proposes a new routing protocol which considers security as a routing metric. In addition, the delay based channel cost metric and probability of presence or absence of LU metric are also considered to establish more reliable and stabilized path.

To minimize the route maintainable cost and route establishment time, this work proposes different weight based routing protocol which considers the trust value of nodes in order to determine most securable path.

2. RELATED WORKS

All material on each page should fit within a rectangle of 18 x CRN is one of the promising network technologies in the era of wireless communications. But it is more vulnerable to multiple attacks and providing security to the PUs becomes major challenge. Majorly, security needs to be provided during spectrum sensing stage and information transmission stage. Here, it discussed several past research works related to secured routing algorithms or protocols. Venkanna *et al.* [11] evaluated the performance of several CRN routing protocols like Spectrum Aware on Demand Routing Protocol (SORP), Spectrum Aware Mesh Routing in Cognitive Radio Networks (SAMER) and Dynamic Source Routing (DSR) with and without blackhole attack using various performance parameters like Throughput, E2E delay and Packet delivery ratio.

Reddy *et al.* [12] proposed an integration of Secure Hash Algorithm-1 (SHA-1) and Soft Computing (SF) method based neural network to avoid the PUs emulation attack. The Received Signal Strength (RSS) and Direction of Arrival (DoA) are used to achieve the localization between the PUs and SUs. Their main objective is to minimize the loss ratio during the communication process. However, they didn't consider the channel availability and security of the LU.

In order to find the intrusion less route to destination, Jaganathan *et al.* [13] suggested a bio-inspired routing protocol to enhance security and routing efficiency which will result in reduced delay cum energy consumption. They proposed Bee Inspired Secured Protocol (BISP) for routing in CRAHNs which focuses on increasing the security before sending data packets and decreasing the overall delay. An instinctive characteristic of Bees towards searching for food is utilized to design the routing protocol which selects the better path to destination. To enrich the security during data transmission, Rivest Shamir Adelman algorithm is applied. Their protocol analyzes the security level of the route and neighbor node energy level before sending the data. However, they didn't detect the malicious behavior of a node during spectrum sensing process.

Khasawneh *et al.* [14] proposed a collaborative approach during spectrum sensing process. It monitors the behavior of sensing nodes and identifies the malicious and misbehaving sensing nodes. They measured the node's sensing reliability using a value called belief level. All the sensing nodes are grouped into a specific number of clusters. In each cluster, a sensing node is selected as a cluster head which is responsible for collecting sensing-reputation reports from different cognitive nodes about each node in the same cluster. The cluster head analyzes information to monitor and judge the nodes' behavior.

Akter *et al.* [15] proposed protocol which accommodates the dynamic behavior of the spectrum availability and selects a stable transmission path from a source node to the destination. They Outlined as a weighted graph problem and then proposed a protocol which measures the weight of an edge by measuring the mobility patterns of the nodes and channel availability. The mobility pattern is defined in the view of distance, speed, direction, and node's reliability. Besides, the spectrum awareness is measured over the number of shared common channels and the channel quality. Even though the authors proposed secured reactive routing protocol, they were not concentrated on the security of the LU during the spectrum sensing.

In order to provide the secure communication, khan *et al.* [16] suggested an algorithm which computes the distrust value to detect the malicious nodes. They improved the network performance but not focused on security of the node while routing of the node towards destination. Further, Idoudi *et al.* [17] proposed a cluster based scheduling algorithm which considers sensor energy. They also discussed the collision of the CR nodes in the clusters to provide the better communication among the nodes. Further, energy efficient routing protocol is introduced by Cladia *et al.* [18] which were implemented optimized dijkstra algorithm to avoid interference of LU user in channel switching.

Srikanth and Sudhir [19] proposed an optimal trusted intrusion detection system for considerate spectrum sensing and distribution in CRNs (OT-IDS-CR). They, initially introduced an improved chaos butterfly optimization (ICBO) algorithm for efficient clustering which divide the sensing nodes into number of clusters. Later, they computed the trust degree of each SU based on sensing information with the help of cooperative random learning based trust management system (CRL). Then, they utilized the multi-swarm biogeography optimization (MBO) algorithm to optimize the sensing information's to avoid the dimensionality problem and to ensure the secure spectrum sensing and allocation. However, they didn't consider the nodes' behavior to provide the secured routing. To select the feature of a node using Support Vector Machine (SVM) and to find the route to destination in an optimized manner, Jaganathan and Ramkumar [20] proposed Meticulous Elephant Herding Optimization based Protocol (MEHOP). SVM algorithm is applied to classify the nodes from malicious node. MEHOP isa metaheuristic algorithm designed to make updating from the selected individuals. Once when the intrusions are detected and avoided, the performance of the ad-hoc network gets improved.

Kumari *et al.* [21] introduced an efficient malicious node detection system in CRNs. Their system contains features extraction and optimization with soft computing framework. They initially abstracts the features of each individual node in CRN and the individual features are optimized using feed forward radial neural network algorithm, which differentiates each individual node in CRN into either normal or malicious/faulty. They evaluated the performance through malicious node detection rate, throughput and latency. However, they have not discussed the malicious behavior of LU.

Salameh *et al*. [22] suggested a security-aware routing protocol that considers jamming attacks which interrupt cognitive radio transmissions. A most secure channel is assigned for each hop within an IoT source-destination pair in accordance to an optimization problem. Moreover, since CRNs are more vulnerable to threats, an Ensemble-based Jamming Behavior Detection and Identification (E-JBDI) technique is proposed as a second line of defense. It is used to identify the behavior anomaly of jamming attack. Mostly, the authors considered the security of the channel and not on the nodes' behavior.

Further, Zhong *et al.* [23] proposed energy and trust aware OR (ETOR) in CR-Social Internet of Things (SIoT), which jointly considers energy efferent, trust and social feature. They exploited a new routing metric for selecting forwarding candidates and use network coding for the data transmission between trust nodes in multiple types of flows SIoT. In addition, they proposed a game-theoretic approach to allocate channel for SIoT which is based on interference factor.

Salameh et al. [24] introduced a new jamming-aware routing and channel assignment protocol that deals with proactive jamming attacks in CR-based IoT networks without requiring extra resources. Their protocol attempts at improving the overall packet delivery ratio in the network while considering the PU's activities, multi-channel fading and jamming behavior. Their protocol consists of three phases: route discovery, channel assignment, and path selection. The channel assignment problem along each path is formulated as an optimization problem with the objective of maximizing the end-to-end probability of success. Even though, the authors considered the security of LU but not on the malicious activities of all nodes.

Vivekanand *et al.* [25] presented a Secure Distance based Improved LEACH Routing (SDILR) protocol to avoid the primary user emulation attack (PUEA) in CRN. Initially, the nodes in the CRN are clustered by using distance based improved Low- energy adaptive clustering hierarchy (ILEACH). After the formation of clusters, secure routing is presented using support value based signature authentication to avoid PUEA. Next, Prasanna Venkatesan *et al.* [26] proposed a secure and reliable routing in CRN based on distributed Boltzmann–Gibbs learning algorithm. They implemented for relay node selection phase. In addition, the authentication is done based on secure routing distributed Boltzmann–Gibbs learning algorithm. They considered the metrics namely trust value and total delay for the successful and reliable transmission of the packet. Further, to increase the reliability, they implemented LDPC code at the time of relay node selection phase. The proposed code helps to cancel any kind of electronic interference and channel noise interference but not completely considered the security during spectrum sensing.

Further, Energy efficient collaborative spectrum sensing (EE-CSS) protocol based on trust and Reputation management is proposed by Elanagai and Jayasri [27]. Trust and reputation management system (TRMS) have been proposed to combat malicious behavior in CRN. TRM unit Calculates the Trust Value for each Secondary User's and find out the attacker nodes and drops them out from the network. EE-CSS protocol improves the Energy Efficiency by Reducing the Total Number of Local decisions i.e. sensed energy level, between SUs and its Fusion Centre. Since each sensing report requires energy for transmission, processing and receiving it must be reduced to improve energy efficiency. This CR Network is subjected to two varieties of routing protocols such as AODV and Hybrid Routing Algorithm. Singh *et al.* [28] introduced a Trust based Intelligent Routing Algorithm which exploits the Call Data Record from Call Detail Record. The function of Artificial Neural Network is to calculate and learn, trust value that can be shared among network devices. This algorithm lowers the need of nodes resources like energy consumption, computation time and space overheads. Their algorithm enhances the routing performance in DTN and provides an in-built security without any additional overhead.

From the security perspective, a Malicious User (MU) may imitate the PU signal with the intention to never allow the CU to use its idle band, which ultimately degrades the overall network performance. Attacks like Cognitive User Emulation Attack (CUEA) and Primary User Emulation Attack (PUEA) may get encountered by the handoff procedure that needs to be resolved. To address this issue, Rathee et al. [29] proposed a secure and trusted routing and handoff mechanism specifically for the CRN environment where malicious devices are identified at the lower layers, thus prohibiting them from being part of the communication network. Further, at the network layer, users need to secure their data that are transmitted through various intermediate nodes. To ensure a secure handoff and routing mechanism, a Trust Analyzer (TA) is introduced between the CU nodes and network layer. The TA maintains the record of all the communicating nodes at the network layer while also computing the rating and trust value of the Handoff Cognitive User (HCUs) using the Social Impact Theory Optimizer (SITO)..

3. PROPOSED METHODOLOGY

This section explores the details of basic system model, node's malicious behavior and secured routing mechanism. The proposed methodology is divided majorly into two phases; they are malicious nodes detection and secured path determination. The malicious node is detected based on the trust value and availability of the spectrum. Further, the secured path is determined based on the cost of each node which includes inverse of Trust Value (TV), channel cost, and probability of presence of PU or LU.

3.1 System Model

The proposed system model is shown in the Figure.1. Here, it consider a network which consists of *C* number of SUs and they are partitioned into *P* number of clusters by considering the metrics such as channel availability, geographical locations, channel quality, signal strength, and node degree [30]. Here, one TV is assigned to each CU which is used to evaluate the node's reliability and accuracy in concern with security. The entire network's traffic is controlled by one entity called as Fusion Centre (FC) which also manages the communication among the clusters. Further, the FC choses a node with highest TV as Cluster Head (CH) in each cluster. Here, it assume that no node become malicious once it is selected as a CH [31]. The proposed method mainly concentrates on to detection of the malicious behavior of a CU during spectrum sensing stage.

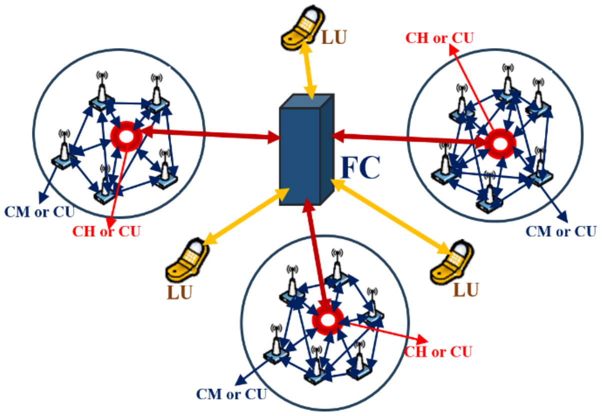

Fig 1: System Model

Initially, at the time of joining, each node is assigned with moderate TV of 2 which indicates the trusted node. Here, different trust categories are considered to evaluate the trustworthiness of each node, as shown in Table.1. Initially, a random node is selected as a CH at the time of cluster construction since entire nodes have equal TV. The CHs selection is rotational basis, when the new node is added and it has high TV than the current CH trust value, then it is selected as a new CH. Further, it assume that energy detection technique is used to sense the unutilized spectrum by all CUs. The proposed method concentrates only on the analysis of spectral sensing but not on the type of spectrum sensing. Further, Cooperative spectrum sensing is used where spectrum is sensed by all Cluster Member (CM) nodes, decision taken about the absence or presence LU, and finally the decision was forwarded to all its neighbor nodes. Next, each neighbor node prepares a report called as Sensing Estimation Report (SER) after receiving sensing decision and this report is transferred to the

CH. Here, it propose a new secured routing mechanism that is not only considered each CU's trust values but also the probability of presence of LU and cost of the channel. Here, cost of the channel is measured in terms of delay.

Table 1. Trust Categories

Trust Value (TV)	**Category of the Trust**
0 ≤ TV ≤ 1	Most Untrusted
1 < TV < 2	Untrusted
2 ≤ TV < 3	Trusted
3 ≤ TV ≤ 4	Very Trusted

3.2 Malicious Nodes Detection Mechanism

Each CU in every cluster senses the spectrum to determine the unutilized spectrum. Here, energy detection spectrum sensing method is used to detect the absence or presence of LU based on the signal strength [32]. The sensed information is compared with available past known LU's signal information which is stored in the specific LU's channel to detect the behavior of a CU that is malicious or not. If both the signals are matched, then there is an active LU in its spectrum channel otherwise there is a malicious node which emulates the LU. If there is no signal is received in the channel, then there is no active LU and the spectrum is free. Further, this information is broadcasted to its entire neighbor CUs. Further, sensing an unutilized spectrum is a periodic process and it takes several rounds. In each round, every CU must complete its sensing process and store the sensed information for further usage in the parameter called as Sensing Outcome (SO). SO consist of two values namely *0* and *1*; *1* indicates there is a real LU, *0* indicates no real LU. SO of each CU is broadcasted to its entire neighbor CUs in each cluster. Next, each CU receives the SO of its neighbor CUs. Upon receiving, each CU compares its own SO with the neighbor CUs' SO. If it matches, CU creates an opinion about neighbor CU that the corresponding CU is benevolent otherwise it is malicious. Finally, each CU prepares a SER and its format is shown in the Table 2.

Table 2. Trust Categories

Sensing Node ID (SN_{ID})	SO_{SN}	Receiving Node ID (RN_{ID})	Opinion

where, SO_{SN} indicates the sensing outcome of sending node and it is either *0* or *1*. If $SO_{SN}=0$ then there is a free spectrum and if $SO_{SN}=1$ then the spectrum is occupied and opinion indicates the opinion about receiving node and it is either *0* (indicates receiving node is malicious) or *1* (indicates receiving node is benevolent). Like this, each CU prepares SER and forwards it to CH. Next, CH analyses the SER of each CU then makes following final decisions; They are categorized based on the availability of spectrum i.e., occupied or free and the Opinion of each CU i.e., malicious or benevolent.

Further, each CH forwards the final decision to all its CM nodes about spectrum availability and TV. In order to process these reports, specific rule is applied by the CH that is *K-out-of-N* rule. According to this rule, *K* out of *N* users must have same opinion in order to consider their opinion. In case 50% *K*-rule is used, *K=N/2*. Here, it propose a new *K*-rule where *K* represents the number of acquired points. Each CU is assigned with different weighted points based on its TV. The value of *K* can be found based on the TV and its categorization is shown in Table 3.

Table 3. Categorization of *K* based on TV

Trust Value	***K* (Acquired Points)**
0 ≤ TV < 2	0
2 ≤ TV < 2.5	1
2.5 ≤ TV < 3	2
3 ≤ TV ≤ 4	3

Afterwards, number of malicious and benevolent opinions is collected from each CU to update the TV by CH. Then, each benevolent node is rewarded with an increment in its TV and each malicious node is penalized with decrement in its TV. Later, each CH computes one parameter called as Modification Factor (MF) which is defined as the difference between malicious and benevolent opinions about receiving node that are forwarded by the sending nodes. After computing MF from Eq. (1), it is added to past TV to update the current TV of CU. At $t = t_{current}$ the Modification Factor of i^{th} CU is computed as

$$MF_{CU_i} = \left(\sum\nolimits_{b=1,\neq i}^{B} w_r \times norm(TV_{CU_b})\right) - \left(\sum\nolimits_{m=1,\neq i}^{M} w_p \times norm(TV_{CU_m})\right) \quad (1)$$

$$(MF_{CU_i})_{t_{current}} = (MF_{CU_I}) + (\mathrm{TV}_{CU_I})_{t_{PAST}}\ s.t. -4 \leq MF \leq 4 \quad (2)$$

where *B* and *M* represents the number of nodes that decides CU_i is a benevolent node and malicious node respectively, w_r and w_p denotes the rewarding and penalizing weight factors respectively, *norm* represents the normalized *TV* of sending node that forwards the opinion stating that it is a benevolent node. The MF varied between -4 and +4, if MF is greater than 4, then it is adjusted to 4 and if it is lesser than -4, then it is adjusted to -4. The MF value varies based on the TV value of each CU. Greater trust value indicates major effect on MF. After computing final TV, then it is added with other routing Metrics to find out the secured path.

3.3 Secured Routing Mechanism

The proposed secured routing technique choses a best path between any two nodes. Eq. (3) is used to find the best next-hop node among the available neighbor nodes. According to the Eq. (3), current node choses one of the neighbor nodes as a next-hop node that has maximum TV, minimum channel cost, and minimum probability of presence of LU, mathematically it is expressed as

$$f = \max(TV_{CU_j}) + \min(ch_{\mathrm{cost}}) + \min(P_{LU}) \quad (3)$$

where, *f* represents the function for finding the best next-hop node, TV_{CU_j} denotes the trust value of CU_j, ch_{cost} represents the channel cost that is delay, and $\mathrm{P_{PU}}$ denotes probability of presence of LU. According to the Eq.(3), initially every CH transmits accumulation of TV of next-hop node(s), probability of presence of LU over the channels, and delay based channel cost to its CM nodes. Next, each current node (CU_i) computes the inverse of TV of next-hop node (CU_j) i.e., $TV_{CU_j}^{inverse} = 1/TV_{CU_j}$. Further, along with $TV_{CU_j}^{inverse}$, ch_{cost} and P_{PU} are stored into next-hop node information table and it is shown in Table 4.

Table 4. Next-hop Node Information

Next-hop Node ID	Inverse of TV	Cost of the Channel	Probability of presence of LU

Table.4 is used to compute next-hop node's information and also for the determination of best next-hop node among the available neighbor nodes. Using the above Table 4, each CU maintains next-hop node's information. Then, the nodes are arranged in order for each parameter by CU, and each node is given a number that denotes its position in relation to the other nodes. Finally, the cost of the next-hop node is evaluated by multiplying nodes' order of each parameter with its weight value. Therefore, one node is selected as best next-hop node among the neighbor nodes which has minimum cost and it is expressed in the following Eq. (4),

$$f(C_{NN}^{\min}) = MIN\begin{pmatrix}\left(\alpha\times order(TV_{CU_j}^{inverse})\right)+\\ \left(\beta\times order(ch_{\text{cost}})\right)+\\ \left(\gamma\times order(P_{LU})\right)\end{pmatrix} \qquad (4)$$

Where, $f(C_{NN}^{\min})$ is the function which has minimum cost of the next-hop node *α, β* and *γ* represents the weight values of $TV_{CU_j}^{inverse}$, ch_{cost} and P_{LU} respectively. The weight values are assigned is such a way that the best secured path should be selected. The highest weight value is assigned for trust value metric i.e., α =0.5 , followed by probability of presence of LU i.e., , *β= 0.3* then channel cost i.e., *γ* =0.2 and always they should maintain $\alpha + \beta + \gamma = 1$.

4. SIMULATION ANALYSIS

This section describes the performance validation experiments for proposed research work. Here, the proposed work is compared with state-of-the art methods such as SHA-SF [12], and BISP [13]. Here, it considered the network area of 200m*200m, the number of nodes are 50, and the number of radio channels are 20. Further, assumed the rewarding weight factor w_r*=0.3* and penalizing weight factor w_p*=0.7*. The remaining simulation parameters are listed in Table.5. The performance is evaluated in three different cases: effect of number of CUs, effect of number of malicious nodes, and effect of number of available channels. In each case packet delivery ratio, packet loss ratio, and end-to-end delay performance metrics are computed and compared with existing methods such as SHA-SF [12], and BISP [13]. It also measured the performance metrics like malicious detection rate, false positive rate, and control overhead.

As number of malicious nodes increases, the number of routes will decrease due to multiple attacks then number of packets exchanging also effects. Figure.2 shows the packet delivery ratio with varying number of malicious nodes. From the results, it observe that as number of malicious nodes increases packet delivery ratio decreases. The proposed work achieves better packet delivery ratio than the existing methods due to the efficient malicious nodes' detection. The proposed work detects the malicious nodes based on the trust values, if any node has lower trust value, then it is terminated from the path and the packets are delivered through non malicious routes. Further, it observe that on and average the packet delivery ratio for proposed method is approximately 81.33%, SHA-SF is 55%, and BISP is 34.16%..

Table.5 Simulation Setup

Parameter	**Value**
Number of Nodes	50
Number of Radio Channels	20
Size of packet	512 bytes
Type of channel	Wireless channel
Type of MAC	IEEE 802.11e
Model of Antenna	Omni Antenna
Propagation model	Free Space
Application protocol	FTP
Number of SUs	[10 20 30 40 50]
Number of Malicious Nodes	(10-50) % of Total Nodes in Network
α	0.5
β	0.3
γ	0.2

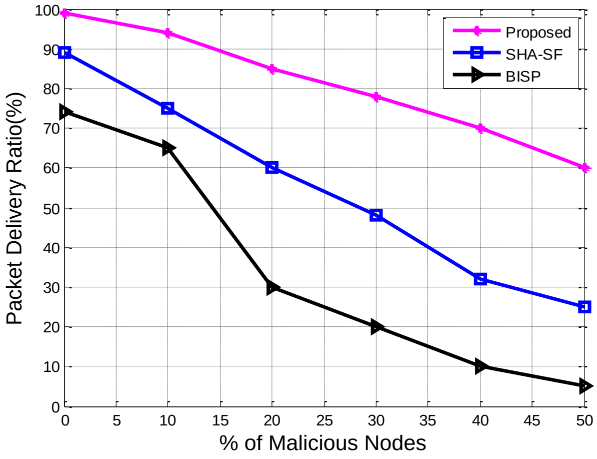

Fig 2: Packet delivery Ratio Comparison with varying malicious node count in the Network

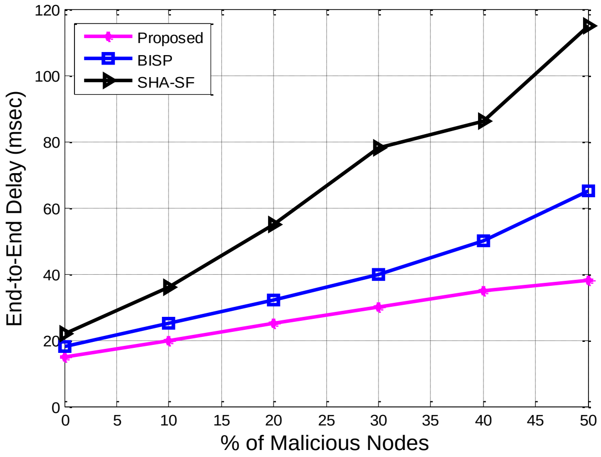

Fig 3: End-to-End Delay Comparison with varying malicious node count in the Network

Figure.3 shows the end-to-end delay with varying number malicious nodes. There is a direct relation between the end-to-end delay and % of malicious nodes i.e., as number malicious nodes increases the end-to-end delay also increases. However, the proposed work has lower end-to-end delay than the existing methods because the route which contains malicious nodes is excluded based on the trust value of the node. As number of malicious nodes increases, the number of routing paths decreases due to number of multiple attacks but the proposed mechanism selects most secured routes to deliver the packets. So, the packet delivery takes less time than the existing methods. It observe that the approximated average end-to-end delay for proposed work, BISP, and SHA-SF are 27.16ms, 39ms, and 66.16ms respectively.

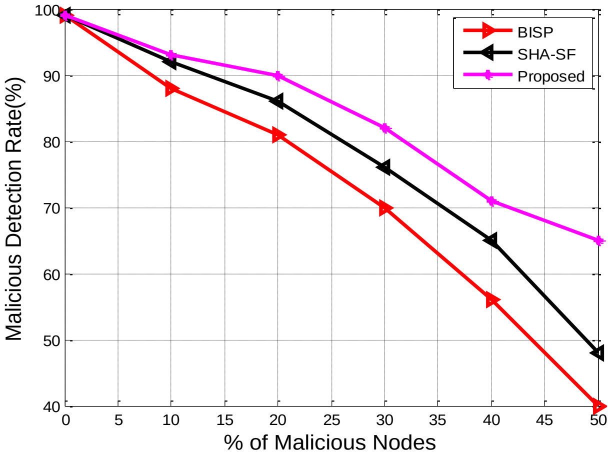

Fig 4: Malicious Detection Rate comparison with varying malicious node count in the Network

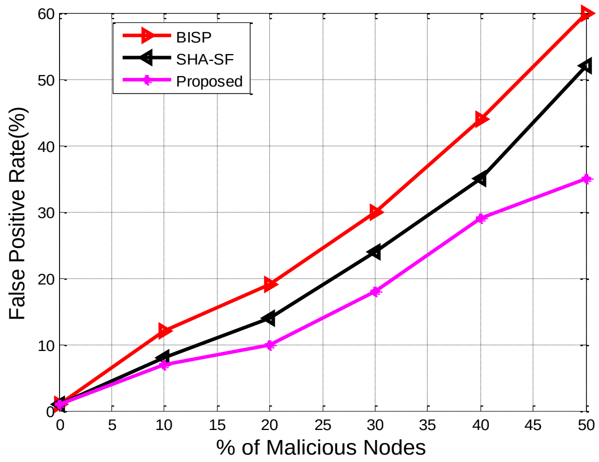

Fig 5: False positive Rate comparison with varying malicious node count in the Network

Figure.4 shows the Malicious Detection Rate comparison with varying malicious node count in the Network. From the observations, it can see that the MDR follows an inverse relation with % of malicious nodes. As the number of malicious nodes increases in the network, they get compromised with different attacks. in such condition, a single methodology can't identify all the attacked nodes. However, the proposed method has experienced more MDR because it involved the CR attributes into routing metric. On an average, the proposed method has gained the MDR of 86.5231% while the existing methods SHA-SF and IBSP have gained only 75.6312% and 70.2220% respectively. Similarly, the Figure.5 shows the False Positive rate comparison with varying malicious node count in the Network. The MDR follows an inverse relation with MDR, as the MDR increases, the FPR decreases and vice versa. Hence, the proposed methods experienced less FPR compared to the existing methods. On an average, the proposed method has gained the FPR of 13.4769% while the existing methods SHA-SF and IBSP have gained only 24.3688% and 29.7780% respectively.

5. CONCLUSION

The scarcity of spectrum can be solved by the effective CR technology. But, the presence of adversary nodes in CRAHN makes the spectrum sensing ineffective and hence the investigation *f* reliability in spectrum sensing is very important. Towards such aim, this paper developed a new secure routing mechanism in CRAHNs called as SSTAR. SSTAR analyzes the node's spectrum sensing behavior and finds an effective neighbor node to establish secure ad trustworthy node. Three parameters namely Trust value, channel cost and probability of presence of Primary user are considered for the computation of trustworthiness. Extensive simulations experiments are carried out over the proposed approach and the performance is assessed through different metrics like packet delivery ratio, packet loss ratio, delay and malicious detection rate for varying count of malicious nodes. The comparison between proposed and existing approaches shows the superiority.

CRAHN is a long-distance communication task via relays that only considers energy-efficient line collection. However, convergence is only supported for short-range communications. Therefore, considering relays for long-distance communication is an obvious future direction to extend this research work.

6. REFERENCES

[1] Li, J., Feng, Z., Wei, Z., Feng,Z., Zhang,P., "Security management based on trust determination in cognitive radio networks", EURASIP Journal on Advances in Signal Processing, Vol. 2014, No. 1, pp. 48, 2014.

[2] Vivekanand, C. V., Bagan, K.B., "Secure Distance Based Improved Leach Routing to Prevent PUEA in Cognitive Radio Network", Wireless Personal Communications, Vol. 113, pp. 1823-1837, 2020.

[3] Elangovan, K., Subashini, S., "Particle bee optimized convolution neural network for managing security using cross-layer design in cognitive radio network", Journal of Ambient Intelligence and Humanized Computing, pp. 1-9, 2018.

[4] Patnaik, M., Kamakoti, V., Matyáš, V., chák, V., "PROLEMus: A proactive learning-based MAC protocol against PUEA and SSDF attacks in energy constrained cognitive radio networks", IEEE Transactions on Cognitive Communications and Networking, Vol. 5, No. 2, pp. 400-412, 2019.

[5] Guo, J., Zhou, X., "Secure distributed routing algorithm with optimizing energy consumption for cognitive radio networks", Wireless Personal Communications, Vol. 72, No. 4, pp. 2533-2550, 2013.

[6] Nguyen-Thanh, N., Ciblat, P., Pham, A. T., Nguyen, V. T., "Surveillance strategies against primary user emulation attack in cognitive radio networks", IEEE Transactions on Wireless Communications, Vol. 14, No. 9, pp. 4981-4993, 2015.

[7] Jararweh, Y., Salameh, H.A.B., Alturani, A., Tawalbeh, L., and H. Song, "Anomaly-based framework for detecting dynamic spectrum access attacks in cognitive radio networks", Telecommunication Systems, Vol. 67, No. 2, pp. 217-229, 2018.

[8] Xin, C., Song, M., "Detection of PUE attacks in cognitive radio networks based on signal activity pattern", IEEE Transactions on Mobile Computing, Vol. 13, No. 5, pp. 1022-1034, 2014.

[9] Karimi, A., Taherpour, A., Cabric, D., "Smart traffic-aware primary user emulation attack and its impact on secondary user throughput under rayleigh flat fading channel", IEEE Transactions on Information Forensics and Security, Vol. 15, No. 1, pp. 66-80, 2019.

[10] Akram, M. W., Salman, M., Shah M. A., Ahmed, M. M., "A review: Security challenges in cognitive radio networks," 2017 23rd International Conference on Automation and Computing (ICAC), Huddersfield, UK, 2017, pp. 1-6, 2017.

[11] Venkataramana B., Jadhav, A., "Performance Evaluation of Routing Protocols under Black Hole Attack in Cognitive Radio Mesh Network," 2020 International Conference on Emerging Smart Computing and Informatics (ESCI), Pune, India, pp. 98-102, 2020.

[12] Reddy, V., Rajagopala, R., Linga, R., Sanjeev, "Detection and Prevention of Primary User Emulation Attack in Cognitive Radio Networks Using Secure Hash Algorithm", International Journal of Intelligent Engineering and Systems, Vol. 14, pp. 136-146, 2021.

[13] Jaganathan, R., Vadivel, R., "Bee inspired secured protocol for routing in cognitive radio ad hoc networks", Indian Journal of Science and Technology, Vol. 13, pp. 2159-2169, 2020.

[14] Khasawneh, M., Agarwal, A.,, "A Collaborative Approach for Monitoring Nodes Behavior during Spectrum Sensing to Mitigate Multiple Attacks in Cognitive Radio Networks", Security and Communication Networks, Vol. 2017, pp. 1-16, 2017.

[15] Akter, S., Rahman, S., Mansoor, N.,, "An Efficient Routing Protocol for Secured Communication in Cognitive Radio Sensor Networks", arXiv:2008.12895, 2020.

[16] Khan, U., Agrawal, S., Silakari, S., "Detection of malicious nodes (dmn) in vehicular ad-hoc networks", Procedia computer science, Vol. 46, No. 9, pp.965-972, 2015.

[17] Idoudi, H., Mabrouk, O., Minet, P., Saidane, L.A, "Cluster based scheduling for cognitive radio sensor networks", Journal of Ambient Intelligence and Humanized Computing, Vol. 10, No. 2, pp.477-489, 2019.

[18] Cladia, A.T., Rajavel, S.E., "December. Optimizing Spectrum Sensing for Energy Efficient Cognitive Radio Sensor Networks", In 2018International Conference on Smart Systems and Inventive Technology (ICSSIT), pp. 333-338, 2018.

[19] Srikanth, A. K., Sudhir, A.Ch., "OT-IDS-CR: Optimal Trusted Intrusion Detection System for Cooperative Spectrum Sensing and Allocation in Cognitive Radio Networks", Eur. Chem. Bull., Vol. 12, No. 5, pp. 2304-2321, 2023.

[20] Jaganathan, R., "Meticulous Elephant Herding Optimization based Protocol for Detecting Intrusions in Cognitive Radio Ad Hoc Networks", International Journal of Emerging Trends in Engineering Research, Vol. 8, pp. 4548-4554, 2020.

[21] Kumari, D.A., "An Efficient Methodology for Detecting Malicious Nodes in Cognitive Radio Networks", Wireless Pers Commun, Vol. 131, pp. 3089-3099, 2023.

[22] Salameh, H. B., Otoum, S., Aloqaily, M., Derbas, R., Ridhawi, I. A., Jararweh, Y., "Intelligent jamming-aware routing in multi-hop IoT-based opportunistic cognitive radio networks", Ad Hoc Networks, Vol. 98, pp. 102035, 2020.

[23] Zhong, X., Lu, R., Li L., Zhang, S., "ETOR: Energy and Trust Aware Opportunistic Routing in Cognitive Radio Social Internet of Things," GLOBECOM 2017 - 2017 IEEE Global Communications Conference, Singapore, pp. 1-6, 2017.

[24] Salameh, H. B., Rawan, D., Aloqaily, M., Boukerche, A., "Secure Routing in Multi-Hop IoT-Based Cognitive Radio Networks under Jamming Attacks", MSWIM '19: Proceedings of the 22nd International ACM Conference on Modeling, Analysis and Simulation of Wireless and Mobile Systems, USA, pp. 323-327, 2019.

[25] Vivekanand, C.V., Bagan, K.B, "Secure Distance Based Improved Leach Routing to Prevent PUEA in Cognitive Radio Network", Wireless Pers Commun, Vol. 113, pp.1823-1837, 2020.

[26] Prasanna Venkatesan, K.J., Vijayarangan, V., "Secure and reliable routing in cognitive radio networks", Wireless Netw, Vol. 23, pp. 1689-1696, 2017.

[27] Elanagai, G., Jayasri, C., "Implementation of network security based data hauling by collaborative spectrum sensing in cognitive radio network", 2017 International Conference on Innovations in Information, Embedded and Communication Systems (ICIIECS), Coimbatore, India, pp. 1-5, 2017.

[28] Singh, A.V., Juyal, V., Saggar, R., "Trust based Intelligent Routing Algorithm for Delay Tolerant Network using Artificial Neural Network", Wireless Netw, Vol. 23, pp. 693-702, 2017.

[29] Geetanjali, Ahmad, F., Kerrache, C. A., Azad, M. A., "A Trust Framework to Detect Malicious Nodes in Cognitive Radio Networks", Electronics, Vol. 8, No.11, pp.1299, 2019.

[30] Yau, K.-L.-A., Ramli, N., Hashim, W., Mohamad, H., "Clustering algorithms for cognitive radio networks: A survey," J. Netw. Comput. Appl., Vol. 45, pp. 79-95, Oct. 2014.

[31] Khasawneh, M., Agarwal, A., "A secure and efficient authentication mechanism applied to cognitive radio networks," IEEE Access, Vol. 5, pp. 15597-15608, 2017.

[32] Khasawneh, M., Agarwal, A., Goel, N., Zaman, M., Alrabaee, S., "Sureness efficient energy technique for cooperative spectrum sensing in cognitive radios," in Proc. Int. Conf. Telecommun. Multimedia (TEMU), Heraklion, Greece, pp. 25-30, Jul. 2012.