Received: September 20, 2023. Revised: November 26, 2023. 634

International Journal of
Intelligent Engineering & Systems

http://www.inass.org/

Cooperative Sensing Assisted Cross layer QoS Assured Routing in Cognitive Radio Adhoc Networks: Ensuring Security and Privacy

Niranjan Muchandi[1]* Rajashri Khanai[1] Mandakini Muchandi[2]

[1]*KLE Dr. MS Sheshgiri College of Engineering, Belagavi, India*
[2]*Gogte Institute of Technology, affiliated to Visvesvaraya Technological University, Belagavi, India*
* Corresponding author's Email: niranjanmuchandi@klescet.ac.in

Abstract: Achieving higher accuracy of spectrum sensing (SS) becomes a challenge in cognitive radio adhoc network (CRAN) due to presence of varied power levels, interference, multipath fading and hidden node problems. Cooperative sensing based SS address these challenges by making spectrum decision based on distributed sensing measurements from multiple nodes. A major problem in cooperative SS is that, false sensing measurements sent by compromised node can impact the spectrum access probability and network services. These false measurements also affect the channel utilization calculation and disrupt the QoS based routing protocols for cognitive radio (CR) networks. The compromised node can also compromise the privacy of SU by leaking communicated messages. In this work, we provide a cross layer QoS assured routing system for CRAN that is secure as well as protects privacy. The proposed solution solves the problems of false sensing measurements using Kolmogorov Smirnov test on spectrum measurements in both spatially and temporal contexts. Attacks on spectrum measurements are detected and filtered using sequential probability test. Cross layer interactions are used in decision on source rate control, multipath selection and adaptive queing to provide guaranteed QoS. The proposed solution is able to increase the spectrum sensing accuracy by at least 7.6% in presence of sensing attacks and increase packet delivery ratio by at least 4% compared to existing works.

Keywords: Cognitive radio adhoc network, Cooperative sensing, QoS, Cross layer.

1. Introduction

CRAN is multi hop data forwarding network with spectrum owned by only certain primary user (PU) and rest of secondary users (SU) opportunistically share the spectrum of primary node when it is available. CRAN is able to solve the problem of limited spectrum availability in application like military communications, vehicular communications etc. Accurate sensing of primary user status is very important for achieving maximum spectrum utilization and throughput in CRAN. SS becomes a challenge in presence of interference, multipath fading, hidden node problems, shadowing effects etc [1]. Many solutions have been proposed to address these challenges [2]. Cooperative spectrum sensing [3] is one such approach in which decision on spectrum availability is based on sensing measurements from multiple nodes. Though cooperative SS is able to address the challenges in SS, it is insecure against spectrum sensing data falsification (SSDF) attack [4]. A compromised node can send false measurements to make the spectrum decision making erroneous. SSDF attack is very common in cognitive networks where PU is paid for sharing the spectrum. Many routing protocols are proposed for achieving a guaranteed quality of service (QoS) in CRAN's. These protocols are based on prediction of channel availability. In presence of SSDF attack, prediction of channel availability becomes erroneous and QoS guaranteed routing fails. Compromised nodes can also leak messages communicated by SU. Towards this end it is necessary to ensure security and privacy in the QoS guaranteed routing protocol for CRAN's.

In this work, a secure and privacy preserving QoS guaranteed routing protocol is proposed for CRAN. The proposed solution uses Kolmogorov Smirnov (KS) test to detect the node launching SSDF attack and filter its sensing measurements in spectrum decision process. Privacy of SU messages is preserved through Shamir secret sharing based data split and forwarding each split in different multi objective optimized QoS path. Following are the contributions of the proposed solution.

- Identification of SSDF attackers by cumulative distribution of spectrum measurements both temporally and spatially using KS test. A cooperative spectrum sensing scheme based on clustering topology is proposed. Spectrum energy measurements over time intervals are matched pair wise at fusion center of each cluster using KS test to detect false measurements and filter them from spectrum sensing decision process. By this way the proposed solution is able to filter the false measurements and increase the accuracy of spectrum sensing.
- Reducing the false positives in malicious node identification using Sequential probability test (SPT). SPT is used to accommodate for transmission failures due to other reasons apart from spectrum availability. By this way, false positive in malicious cluster identification is reduced.
- Privacy preserving multi objective QoS guaranteed routing in CRAN's. The QoS is deteriorated in cognitive networks due to lack of control on data sending rate of nodes based on channel availability and congestion at channels. This is solved in the proposed solution through three novel schemes of source rate control, multipath selection and adaptive queing. The schemes are facilitated through cross layer interaction involving application, physical, transport and link layers. With these three novel schemes, the proposed solution is able to reduce the congestion and increase the packet delivery reliability.

The rest of the paper is organized as follows. The survey on existing works related to spectrum sensing attacks and QoS guaranteed routing is presented in section 2. The research gaps are then identified and detailed. Section 3 presents the proposed cross layer solution to achieve guaranteed QoS. The results of the proposed solution and advantages of proposed solution compared to existing works are presented in section 4. The concluding remarks and future scope of work are presented in section 5.

2. Related works

In [5], proposed a witness based scheme to prevent malicious SU from sending false location information to get access to spectrum in database driven CR networks. The witness SU are initially selected by PU and these witness SU help to authenticate the location provided by any SU to claim spectrum access. Though this solution is not applicable to sensing based CR network, the concept of witness SU authenticating unknown SU's can be used for SSDF detection. The author [6] proposed a modified delivery based scheme to detect malicious secondary users launching SSDF attack. Delivery of packet is attempted and based on the delivery status the decision of any SU is validated. Authors also proposed a mathematical model to estimate the number of delivery attempts to be made to verify the integrity of SU. But delivery attempt failure to other reasons than PU availability is also considered as maliciousness of SU. This increases the false positive rate in this work. In [7] presented a scheme to detect collusive SSDF attacks. The similarity between the sensing measurements of two different SU is measured using XOR distance. The work is based on the assumption that colluding attacks have minimum XOR distance. By this observation, the colluding SSDF attackers are detected. The mechanism works only if all colluding attackers have their sensing time synchronized. In [8], proposed a trust fluctuation clustering analysis to suppress the collusive SSDF attackers. A binary clustering algorithm with similarity distance computation is proposed to group the SSDF attackers. But the method assumes all colluding attackers to behave in similar way and this approach cannot detect multiple groups of collusive attackers. The author's [9] suggested a two level defense scheme called Feed Guard based to prevent collusive false feedback, considerd the concepts of feedback trust and I-C frequency correlation analysis. The method is built based on correlation between the current feedback data and historical sensing data. But false positives are higher in this method. In [10] proposed attacker punishment policy to mitigate the SSDF attacks. This work denies the data transmission schedule to detected attackers in proportion to the number of fake sensing reports they provide, by this way attackers are forced to remain normal. But even a compromised node's only intention is to disrupt the network and doesn't need any data transmission schedule, this scheme fails. The author [11] designed a linear weighted technique to get rid the effects of

SSDF attackers on the sensing decision. Based on the degree of result consistency and the degree of data divergence, a weight is given to each SU user. To distinguish between malicious and trustworthy sensor nodes, an adaptive reputation evaluation is introduced based on the weight. The model scores a SU based on correlating his sensing results to the data transmission results. But the scheme does not have provision to adjust for data transmission failure due to other reasons like receiver not available etc. In [12], proposed a shifting and evaluation trust management algorithm to secure against SSDF attackers. The attackers are detected by observing the sensing report over certain time slots. Genuine SU are rewarded with more transmission slots and malicious SU are punished. The solution works only for single PU. The author's [13] presented an innovative trust management system to assess each SU node level of trust. The reputation of SU is based on numerous elements like history based trust, active factor, incentive factor and consistency factor. Malicious users are excluded from the decision-making process and filtered based on reputation. The technique doesn't take collusion among malicious nodes for launching SSDF attack. In [14], suggested a correlation-based strategy to find SSDF attackers. To identify any unusual SUs, the sensing decisions of each SU are compared to those of other SUs. To categorise the outliers, a box-whisker plot is utilised. However the scheme works for only one PU. In [15] the author suggested a QoS routing protocol that would choose a unique channel at each hop and route according to the needs of the service. The work considered delay and SU-PU interference are recognized as the QoS metrics. Under SSDF attack the SU-PU interference calculation becomes erroneous and this effects the efficiency of QoS routing protocols. In [16], the author proposed a method to exclude malicious SU from sensing decision. Credit value is calculated for SU and SU with credit less than a threshold are filtered out from the sensing decision. But the approach works for only PU. In [17], presented a double adaptive thresholding technique to identify malicious users. Fair chance is provided to doubtful users by using double adaptive threshold test. Any user who fails this test and creates suspicion is labelled as malicious user. Dempster-Shafer evidence theory is used at fusion center to integrate the results of legitimate users. Double adaptive thresholding does not work under collusion attack. The author's [18] computed the credibility of SU based on past behavior, entropy of reported data and SNR. However the approach is not scalable. The time complexity for credibility calculation grows exponential with increase in number of nodes. In [19], employed differential evolution (DE) to mitigate the impact of SSDF attack. Threshold for spectrum decision is made dynamic by learning it from optimum coefficient vector using (DE). The decision fusion from SU is done as weighted fusion with weights based on creditability. But the mechanism does not consider collusive attack. In [20], proposed a multi hop routing protocol for CRAN. The QoS is ensured by spectrum maximization scheme in which SU collaborates and transmit in the regions of PU activity. But collaboration becomes a challenge in presence of SSDF attack. In [21] the author proposed a mechanism to improve the QoS in CRAN combing opportunistic geographic forwarding and network coding. Use of network coding reduces the number of effective transmission and thus improves the QoS. But the performance of the solution severely degrades in presence of SSDF attack. In [22], proposed a boosted tree algorithm to minimize the effects of SSDF in SS. Multiple classifiers are trained and ensemble of these classifiers is done to make the spectrum decision. But in presence of collusive SSDF attack, performance of boosted tree is poor. The author [23] used genetic algorithm to generate various combinations of malicious sensing data. Machine learning classifier is then trained with the generated sensing data to detect malicious users. A weighted fusion rule is followed for spectrum decision with weights allocated based on results of machine learning. The method does not consider the presence of multiple PU channels. In [24], proposed a secure and reliable routing in CRAN's. Trust value of node and total delay through the node are considered as the criteria for next hop selection. To improve the reliability of the packet, LDPC code is used. In presence of SSDF attack, delay calculation becomes erroneous and thus the QoS of routing path is affected. The author [25] suggested a unique hybrid routing system based on on-demand clusters to boost packet delivery ratio (PDR) and decrease delay in CR networks. The nodes are divided into clusters based on spectrum availability, node power levels and node stability. Spectrum availability determination becomes challenging in presence of SSDF attack. In [28], exploited the cross layer design to create effective QoS routes in CR mobile adhoc networks. Cross layer feedback collected in terms of residual energy, PU usage etc are used to select the energy efficient routes. In [29] the author presented a probabilistic multipath cognitive cross-layer routing. MAC layer collects spectrum hole information and passes to application layer to decide channel to use. In [30] a multi-metric cognitive routing protocol has been put forth by cross-layer prospect. Metrics collected at different layers are passed in cross layer

interconnect. But these works did not consider co-operative SS, due to which their gains were limited. The author [31] proposed an imperfect spectrum sensing based multi hop clustering protocol for cognitive radio sensor networks. The solution proposed in this work used energy based spectrum sensing similar to this paper work, but the scheme was not resilient to spectrum sensing attacks. The relays for routing were selected only based on spectrum availability without considering the collision and hence the packet reliability is lower. In [32], proposed a cross layer based generic routing framework to achieve higher throughput and lower delay in cognitive radio networks. The solution combined lower layers for time variant channel estimation. Based on the channel estimation, robust routing path with less PU interference and higher stability is selected. The channel estimation proposed in this work is not resilient against spectrum sensing attacks. The author [33] proposed stability based multipath routing protocol for cognitive radio networks. Unique sensing technique combining energy level with waveform detection is proposed for idle spectrum detection in this work. But the scheme is not resilient against spectrum sensing attacks. The routing is made robust by selecting of path with higher stability. Due to use of multipath, the overhead is higher and the approach did not consider congestion and its impact on QoS on the routing paths. The author [34] proposed a high probabilistic transmission efficiency multi hop routing protocol for CRN. Authors proposed a novel link metric to characterize the transmission efficiency. The routing path with higher link metric is then selected for routing. The link metric proposed in this work considered only transmission distance and channel rendezvous delay. It did not consider the collision on links. Also the spectrum sensing scheme used in this work is not resilient against attacks.

From the survey, we find there is no QoS guaranteed routing protocols for CRAN addressing the problem of channel availability errors due to SSDF attack and mitigating the effects of SSDF attack on QoS of routing path. Also existing cross layer routing protocols have not considered cooperation based SS. Due to this there is higher false positive in SS and this distorts the QoS of the network. The proposed work addresses this problem.

3. Proposed methodology

The solution considered in this work is for clustered topology. The entire network is divided into M × M zones. The fusion centre (FC) for each zone is selected as a node close the zone's centre. In each cluster a node close a four corner are selected a spectrum monitoring nodes (MN). The spectrum monitoring nodes reports their measurements to the FC. FC makes the decision about availability of PU channel based on these measurements. The major notations used in subsequent equations are documented in Table 4.

FC makes the decision by averaging the square of individual measurements as below

$$M_i = \frac{1}{N_x}\sum_{t=0}^{N_x-1}|m_i(t)|^2 \quad (1)$$

In the above equation m_i individually measurement from nodes and N_x is the number of measurement nodes. Each monitoring node sends the measurements to FC for analysis in a sequential manner. From the measurements sent by the monitoring nodes, an energy vector is created for observation in the FC. The SS at each monitoring node is a binary hypothesis test given as

$$H_0: y_i(t) = \eta_i(t)\ , when\ PU\ is\ absent \quad (2)$$

$$H_1: y_i(t) = h_i x(t) + \eta_i(t)\ , when\ PU\ is\ present \quad (3)$$

Where t=1,2,…N_x is the sample index. The total no. of received sample is denoted as η_i.

$$\eta_i = 2BT_s \quad (4)$$

Where B is the predefined bandwidth and T_s is the sensing time. $y_i(t)$ is the received signal at the monitoring $node_i$. x(t) is the transmitted signal by Primary user. Each monitoring node sends it measurements $y_i(t)$ to its FC through a dedicated channel in a sequential manner. The signal is received at cluster head as

$$m_i(t) = \sqrt{PT_i}g_i y_i(t) + \Phi_i(t) \quad (5)$$

Where PT_i is the transmit power of the CRU and g_i is the amplitude gain. $\Phi_i(t)$ is the white Gaussian noise introduced in the transmission. At FC, the received signal is given as

$$m(t|H_0) = \sqrt{PT_i}g_i y_i(t) + \Phi_i(t) \quad (6)$$

$$m_i(t|H_1) = \sqrt{PT_i}g_i h_i x(t) + \sqrt{PT_i}g_i \eta_i(t)(t) + \Phi_i(t) \quad (7)$$

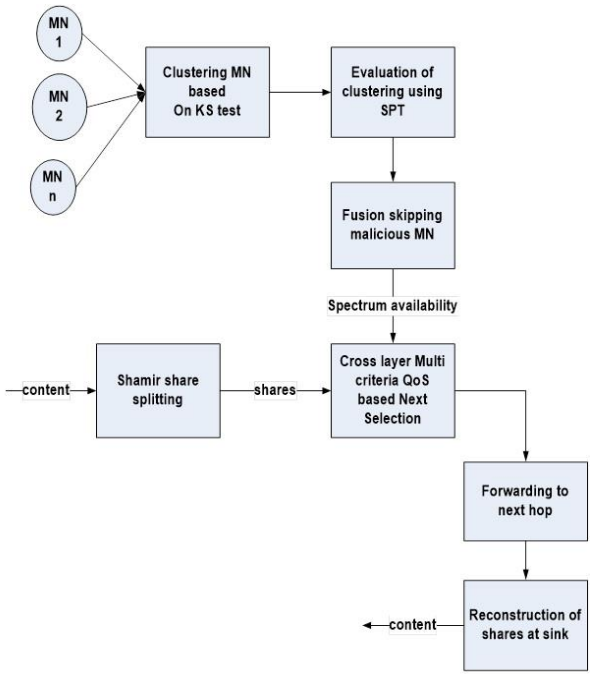

Figure. 1 Architecture of proposed solution

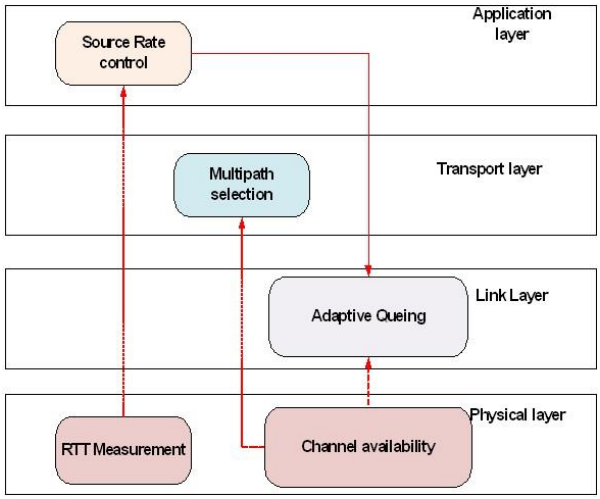

Figure. 2 Cross layer interaction in proposed solution

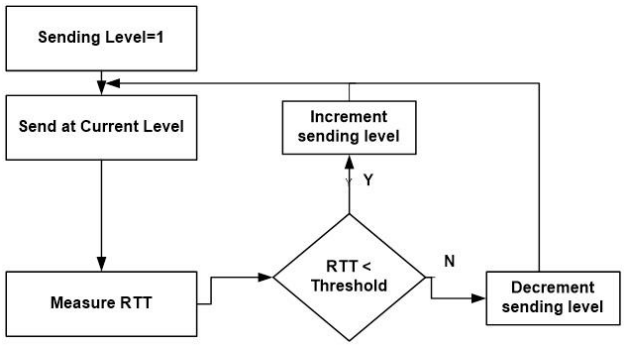

Figure. 3 Source rate control

The architecture of proposed solution is given in Fig. 1. The monitoring node in the clustered topology model can be compromised to send false sensing results. The false sensing results from the compromised node can be one of the following as in Table 1.

Table 1. Cases of false spectrum sensing

Case 1	The measurement corresponding to PU present even though PU is not using the spectrum
Case 2	The measurement corresponding to PU absent even though PU is using the spectrum
Case 3	The measurement corresponding to PU present always
Case 4	The measurement corresponding to PU absent always

In the proposed model, each FC makes sensing decision based on measurements from its monitoring nodes. The energy observed at each monitoring node over K intervals are treated as time series and matched pair to pair if they are drawn from same distribution using Kolmogorov Smirnov test [26]. To determine whether two sets of data are from the same distribution, a non-parametric test is used. The maximum absolute difference between the cumulative distribution functions of two time series, f(x) and r(x), is given as

$$D = \max_{-\infty \le x \le +\infty} |f(x) - r(x)| \quad (8)$$

The probability of similarity of two data samples as

$$prob(D) = Q_{KS}[(\sqrt{N_e} + 0.12 + \frac{0.11}{\sqrt{N_e}})D] \quad (9)$$

Where

$$N_e = \frac{N_1 N_2}{N_1 + N_2} \quad (10)$$

Where N_1 is the no. of samples in series f(x) and N_2 is the number of samples in series r(x).

Q_{KS} is the Kolmogorov Smirnov probability distribution function given as

$$Q_{KS}(\lambda) = 2\sum_{j=1}^{\infty}(-1)^{j-1}e^{-2j^2\lambda^2} \quad (11)$$

When $\lambda = 0$, $Q_{KS}(\lambda) = 1$ while $\lambda = 1$, $Q_{KS}(\lambda) = 0$. The probability of similarity prob(D) is close to 1 when the cumulative distribution function of two time series resemble one other. In cases where the cumulative distribution function of two time series is different, the probability of resemblance prob(D) is nearly zero. By measuring $Q_{KS}(\lambda)$ for all combinations, the monitoring nodes in a zone are grouped in different clusters. Say there are M clusters, the fusion center jointly evaluates all monitoring

node in each cluster at once for their honesty. Each cluster is evaluated as below

Spectrum available decision is based on the energy measurements of monitoring node in the cluster.

- Transmission is attempted and spectrum availability decision is validated using SPT. SPT is used to accommodate for transmission failures due to other reasons apart from spectrum availability. By this way, false positive in malicious cluster identification is reduced.

Sequential probability test tries to prove one of the following hypothesis
H0: Cluster items are honest
H1: Cluster items are malicious
This work employs two thresholds A (higher) and B (lower) based on false positive rate α and false negative rate β to demonstrate the hypothesis as follows

$$A = \log\frac{\beta}{1-\alpha} \tag{12}$$

$$B = \log\frac{1-\beta}{\alpha} \tag{13}$$

The tolerant value for α , β is set by the sink.
The log probability for a node x for T tests is given as

$$P(x) = \log\frac{\prod_{t=1}^{T} P_1(S_t)}{\prod_{t=1}^{T} P_0(S_t)} \tag{14}$$

Following observations can be made based on P(x).

If P(x)<A, then hypothesis H0 can be accepted, and the test can be terminated for node x.

If P(x)>B , hypothesis H1 can be accepted and the test may be halted for the cluster x. In this case, FC marks all monitoring nodes as malicious.

For $A < P(x) < B$, both of the hypothesis cannot be confirmed at this time and cluster x requires additional testing.

Fusion center drops the monitoring nodes from the malicious cluster in the process of sensing decision and uses only the monitoring nodes from legitimate cluster for fusion process.

An on-demand cross layer QoS guaranteed privacy preserving routing is proposed in this work. The proposed protocol combines multiple metrics. The routing is solved as a multi objective optimization function that finds the route from any source to the sink node by simultaneously minimizing end to end delay, hop count and maximizing data rate at each hop. The data rate is maximized by selecting the best channel in each cluster.

At each FC of the zone, the approximate number of hops to the sink node is calculated as

$$N_h = \frac{\sqrt{(x_r - x_t)^2 + (y_r - y_t)^2}}{R} \tag{15}$$

Where (x_r, y_r) is the location of the hop node (x_t, y_t) is the location of the sink and R is the communication range of the node. At each FC a preference factor (PF) is calculated as

$$PF = w_1 * q + w_2 * \frac{1}{N_h} + w_3 * P_o \tag{16}$$

Where w_1, w_2, w_3 are the weights with $w_1 + w_2 + w_3 = 1$
q is the channel quality value calculated as

$$q = \frac{E_{off}}{E_{off}+E_{on}} \times \frac{E_{off}}{max_{k=1\ldots M} E_{off}} \tag{17}$$

Where $\max_{k=1\ldots M} E_{off}$ indicates the maximum expected channel OFF time on all possible channels between the node and the relay. A larger value of q indicates the channel quality is good.
N_h is the approximate number of hops from node to sink.
P_o is the outrage probability of channel

$$P_o = 1 - exp\left(-\frac{\beta N_o d^{\gamma}}{G}\right) \tag{18}$$

Where β is the received SNR, N_o is the mean of the AWGN, d is the distance between the cluster, G is the transmit power at source and γ is the path loss exponent

Source node sends the data to its FC. FC node calculates the PF for its neighboring zones and select the zone with higher PF as the next hop which has not been used last time T times and forwards the packets to that zone. The process is repeated till the packet reaches sink.

To ensure the privacy of the content transmitted from source to sink, the contents are split to N shares with T+1 as the minimum number of shares to reconstruct. Only T shares are allowed to pass through same next hop, due to which, it becomes difficult for any compromised node to reconstruct the content from the shares. Use of Shamir secret sharing also increases the reliability of content delivery as even if a minimal T+1 shares is delivered to sink, it is still possible to reconstruct the data at sink.

Table 2. Cross layer interconnect in proposed solution

Layers	Purpose
Application layer and Physical layer	Source rate control of application layer based on delay feedback from physical layer
Physical layer and transport layer	The number of shares to be propagated in paths is decided at transport layer based on feedback from physical layer.
Application layer, physical layer and link layer	The feedback from application and physical layer is used at link layer to make queing decision.

The QoS is deteriorated in Cognitive networks due to lack of control on data sending rate of nodes based on channel availability and congestion at channels. This work uses cross layer interconnect information to solve this problem. The cross layer interconnect used in proposed solution is given in Fig. 2. The cross layer interactions shown in Fig. 2, is explained in Table 2.

The physical layer measures the round trip time (RTT) based on the MAC protocol feedback.

The round trip time is an estimation of delay based on probability of distribution of delay (f) in both directions over a period of time. It is calculated as

$$RTT = \begin{cases} \sum_{i=0}^{\infty} f_i(a).f_i(b) \ , x = 0 \\ \sum_{i=0}^{\infty} f_i(a).f_{2x+i}(b) + \sum_{i=0}^{\infty} f_i(b).f_{2x+i}(a), x > 0 \end{cases} \quad (19)$$

Where a is forward direction and b is backward direction. The source rate of sending packets is split to multiple sending levels. The level is initially set as default level. The level is increased as the RTT is less than threshold value and decreased as the RTT goes above threshold value. By this way, pumping of packet at source level is controlled based on the network condition. As a result, QoS improves and the amount of packets lost in the network is decreased. Fig. 3 shows the source rate control flow. The data is split to T shares and forwarded in the proposed solution. The number of shares to split the number of paths to forward the T shares is ecided based on the channel availability predictions at the physical layer. In a period of time, when the physical layer predictions more than 70% channel availability without congestion, the data are split to only two shares and sent in single path. When channel availability prediction is less than 70% and more congestion is noticed, the data is split to 10 shares and scheduled on multiple paths. The Queue size at link layer is adapted based on both sending rate and channel availability decision. When the channel availability is more than 70% and sending rate is less than manageable level (the level is configured by the administrators) the packets are queued. When channel availability is more than 70% and sending rate is less than manageable level, the sending rate is reduced by factor of 10% every time. By this way, the packets are not lost in the network and queued till the channel availability increases

Table 3. Simulation configuration

Parameters	Values
Number of channels	4
Channel available probability	{0.7,0.3,0.6,0.8}
Number of Pus per channel	16
PU transmission range	250m
Number of CR nodes	200
Number of attackers	10 to 50
CR node data rate	2 Mbps
Buffer size	8 kb
Sensing time	1ms
Channel switching time	1ms
Weight values	w1=0.5 w2 = 0.3 w3=0.2

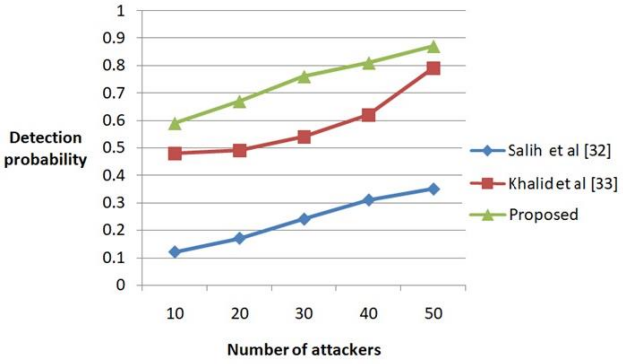

Figure. 4 Probability of detection of attack

4. Results

The proposed solution is implemented in NS2.24 and the simulation is done with configuration given in Table 3.

The performance of the proposed solution in detecting collusive SSDF attack is measured and compared against channel estimation method proposed in [32] and hybrid sensing technique proposed in [33]

The probability of detection of attack is measured by varying attackers (10 to 50) for a fixed 200 CR nodes and the result is given in Fig. 4.

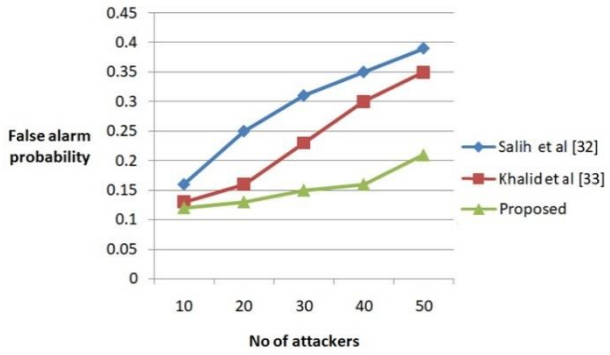

Figure. 5 False alarm probability

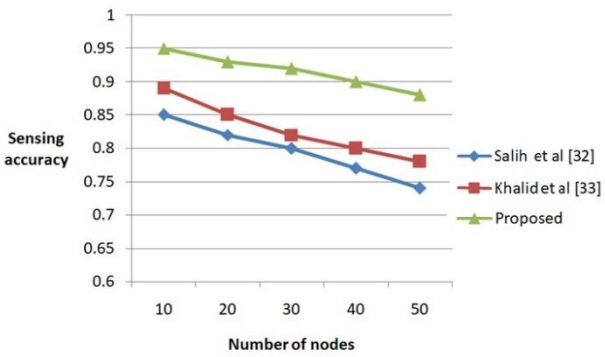

Figure. 6 Sensing accuracy

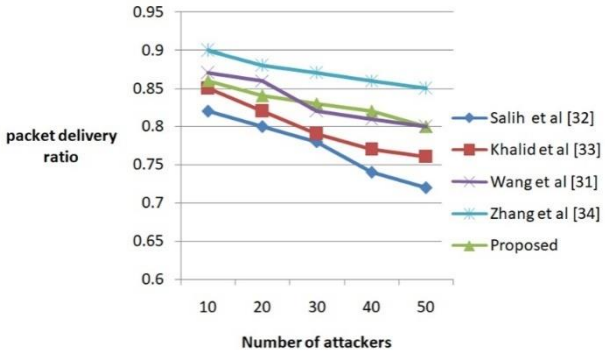

Figure. 7 Comparison of packet delivery ratio

The probability of detection of attack is higher is proposed solution. It is on average 11.08% higher compared to [32] and 21.08% higher compared to [33]. The probability of detection is higher in the proposed solution due to consideration of distribution function of energy measurements and clustering based on KS test results. Joint evaluation of monitoring nodes with SPT further improved the detection rate of attackers in the proposed solution. But in both spectrum sensing schemes of [32] and [33], there were no filtering mechanisms to detect attackers based on their spectrum measurements in both temporal and spatial context. They were able to detect attacks only when spectrum energy measurements crossed the threshold.

The false alarm probability is measured by varying attackers (10 to 50) for a fixed 200 CR nodes and the result is given in Fig. 5.

The false alarm probability is on average 56.57% lower compared to [32] and 98% lower compared to [33]. Use of both KS and SPT has reduced the false positives in the proposed solution. SPT accommodation for transmission failures other than spectrum availability in the proposed solution has reduced false positives compared to [32] and [33]. The false positives were higher in [32] and [33] as they relied only on instant spectrum energy measurements and did not correlate them in temporal and spatial context. But the proposed solution split the networks to clusters and correlated the spectrum energy measurements in both spatial and temporal context.

The sensing accuracy of primary user status is measured for different number of attackers for a fixed 200 CR nodes and the result is given in Fig. 6.

The sensing accuracy is almost 7.6% higher compared to [32] and [33]. The sensing accuracy is higher in proposed solution due to the localization of decision at zone level and relying on multiple monitoring node's measurement for fusion at zone level. Sensing accuracy also increased in proposed solution, due to mitigation of false sensing measurements and attacks using a two stage filtering of KS and SPT tests.

The routing performance of the proposed solution is compared against multi hop routing protocol proposed in [31], cross layer generic routing framework proposed in [32], stability based multi path routing protocol proposed in [33] and multi path routing protocol proposed by in [34]. The performance is compared in terms of

- Packet delivery ratio
- Probability of content deciphering by attacker

The packet delivery ratio is measured by varying the number of attackers for a fixed 200 CR nodes and the result is given in Fig. 7.

The packet delivery ratio is on average 10% higher in proposed solution compared to [32],8% higher compared to [33], 4% higher compared to [31] and [34]. The packet delivery ratio has increased in the proposed solution due to involvement of multiple metrics in next hop selection compared to single

Table 4. Notations used in equations

Notations	Description	Equation number
m_i(t)	Spectrum energy measurement made by a monitoring node i over time t	1
N_x	Number of monitoring nodes making the measurements	1
η_i	Number of samples used for measurement at monitoring node i	4
f(x), r(x)	Two different samples of time series of measurements by two nearby nodes	8
Q_{KS}	Kolmogorov Smirnov probability distribution function	9,11
A	Upper threshold of false positive rate	12
B	Lower threshold of false negative rate	13
N_h	Number of hops from a source node to sink node	15
PF	Preference factor of the link	16
q	Channel quality	17
P_o	Packet outrage probability of a channel	18

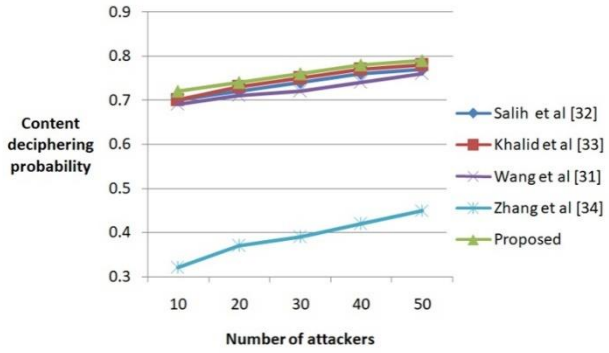

Figure. 8 Comparison of content deciphering probability

metrics for route selection in existing works. [31] selected routing path only based on spectrum availability, [32] selected routing path only based on stability, [33] selected routing path only based on link stability and [34] selected routing path only based on transmission efficiency.

The probability of content deciphering by attacker is measured for different number of attacker and the result is given in Fig. 8.

The content deciphering probability in proposed solution is 34% lower compared to [32], 35% lower compared to [33], 36% lower compared to [31] and 33% lower compared to [34]. The content deciphering probability is lower in proposed solution due to splitting of packets to shares and sending shares in different routes. This reduces the chance of attackers to capture minimal shares and using them to reconstruct the content. But in the existing works, though multi path routing is followed, the packets can be easily deciphered.

5. Discussion

The proposed solution performed better than existing works in three aspects of spectrum sensing, packet delivery ratio and content security. The spectrum sensing accuracy has increased in the proposed solution due to two stage filtering of attacks on sensing measurements using KS and SPT tests. The existing works lacked such protected and relied only on energy measurement threshold to detect false measurements. The second important advantage in the proposed solution is higher packet delivery ratio even at higher attack ratio. The packet delivery ratio has increased in the proposed solution due to source rate control based on network traffic characteristics and selection of more stable paths for routing. Though the existing works selected stable paths, they lacked source rate control. Due to it, the packet drops were higher when collisions occurred. The proposed solution also increased the security of contents by splitting packets according to Shamir share split mechanism. The packets were routed in paths in such a way that minimal share needed for reconstructing contents were never sent in single path. By this way attackers were not able to decipher contents. The existing works did not have such content protection mechanisms.

6. Conclusion

A secure and privacy preserving QoS guaranteed routing protocol is proposed in this work. Collusive and independent SSDF attackers are detected by clustering based on KS test statistics on the energy measurement of monitoring nodes. Due to this false sensing measurements were filtered and the sensing accuracy increased by 7.6% compared to existing works. A multi criteria QoS guaranteed routing based on multiple metrics is used for next hop selection. In

addition source rate is controlled dynamically based on traffic characteristics. Due to this, the packet delivery ratio in the proposed solution increased by at least 4% compared to existing works. In addition, the proposed solution used Shamir secret sharing algorithm to ensure privacy and security against content deciphering attacks. The probability of attackers capturing packets and reconstructing contents is minimized. It is at least 23% lower compared to existing works. Thus the proposed solution performed well in all three aspects of sensing accuracy, packet delivery ratio and content security compared to existing works.

Conflicts of interest

The authors declare no conflict of interest.

Author contributions

The authors confirm contribution to the paper as follows: Study conception, design, Analysis and interpretation of results: Niranjan Muchandi and Rajashri Khanai; Draft manuscript preparation: Niranjan Muchandi and Mandakini Muchandi. All authors reviewed the results and approved the final version of the manuscript.

References

[1] A. Hossain, M. Noor, and R.Azzuhri, "Spectrum sensing challenges & their solutions in cognitive radio based vehicular networks", *International Journal of Communication Systems*, Vol. 34,No. 7,pp. 1-23, 2021.

[2] Y. Arjoune and N. Kaabouch, "A Comprehensive Survey on Spectrum Sensing in Cognitive Radio Networks: Recent Advances, New Challenges, and Future Research Directions", *Sensors (*Basel, Switzerland), Vol. 19, No. 1, p. 126,2019.

[3] A. Ghasemi and S. Sousa, "Collaborative spectrum sensing for opportunistic access in fading environments", In: *Proc. of First IEEE International Symposium on New Frontiers in Dynamic Spectrum Access Networks*, DySPAN, pp. 131-136, 2005

[4] S. Shrivastava, A. Rajesh, P. Bora and B. Chen, "A Survey on Security Issues in Cognitive Radio based Cooperative Sensing", *IET Communications*, Vol. 15, No. 7, pp. 875-905, 2021

[5] R. Zhu, L. Xu, Y. Zeng, and Y. Xun, "Lightweight Privacy Preservation for Securing Large-Scale Database-Driven Cognitive Radio Networks with Location Verification", *Security and Communication Networks*, Vol. 2019, 2019.

[6] K. Yadav, D. Roy and S. Kundu, "Defense Against Spectrum Sensing Data Falsification Attacker in Cognitive Radio Networks", *Wireless Personal Communication*, Vol. 112, pp. 849-862, 2020.

[7] J. Feng, M. Zhang, Y. Xia, and H. Yue, "Securing cooperative spectrum sensing against collusive SSDF attack using XOR distance analysis in cognitive radio networks", *Sensors*, Vol. 18, No. 2, p. 370, 2018.

[8] F. Zhao, S. Li, and J. Feng, "Securing cooperative spectrum sensing against DC-SSDF attack using trust fluctuation clustering analysis in cognitive radio networks", *Wireless Communications and Mobile Computing*, Vol. 2019, 2019.

[9] J. Feng, S. Li, H. Wang and A. Fu, "Securing cooperative spectrum sensing against collusive false feedback attack in cognitive radio networks", *IEEE Transactions on Vehicular Technology*, Vol. 67, No. 9, pp. 8276-8287, 2018.

[10] S. Althunibat, J. Denise and F. Granelli, "Identification and punishment policies for spectrum sensing data falsification attackers using delivery-based assessment", *IEEE Transactions on Vehicular Technology*, Vol. 65, No. 9, pp. 7308-7321,2016

[11] R. Wan, L. Ding, and Z. Xing, "Mitigation strategy against spectrum-sensing data falsification attack in cognitive radio sensor networks", *International Journal of Distributed Sensor Networks*, Vol. 15, No. 9, 2019.

[12] S. Tephillah, J. Martin, and L. Manickam, "An SETM Algorithm for Combating SSDF Attack in Cognitive Radio Networks", *Wireless Communications and Mobile Computing*, Vol. 2020, 9 pages, 2020.

[13] S. Kar, S. Sethi, and K. Sahoo, "A Multi-factor Trust Management Scheme for Secure Spectrum Sensing in Cognitive Radio Networks", *Wireless Personal Communications*, Vol. 97, No. 2, pp. 2523-2540, 2017.

[14] S. Khan, M. Faisal, M. Kim, and S. Ahmed, "A Correlation-Based Sensing Scheme for Outlier Detection in Cognitive Radio Networks", *Applied Sciences*, Vol. 11, No. 5, 2021.

[15] N. Raj, A. Nayak, and S. Kumar, "QoS aware routing protocol for Cognitive Radio Ad Hoc Networks", *Ad Hoc Networks*, Vol. 113, 2020.

[16] H. Du, S. Fu, and H. Chu "A Credibility-based Defense SSDF Attacks Scheme for the Expulsion of Malicious Users in Cognitive

Radio", *International Journal of Hybrid Information Technology*, Vol. 8, pp. 269-280, 2015.

[17] S. Khan, M. Jibran, I. Koo and J. Kim, "A Double Adaptive Approach to Tackle Malicious Users in Cognitive Radio Networks", *Wirel. Commun. Mob. Comput.*, Vol. 2019, Article ID 2350694, 2019.

[18] J. Hwang, J. Kim, I. Sung, D. Yoo, and K. Kim, "Fast and Accurate Detection of Malicious Users in Cooperative Spectrum Sensing Network", *Wireless Personal Communication*, Vol. 118, pp. 1709-1731, 2021.

[19] N. Gul, M. Qureshi, S. Khan, A. Elahi, and S. Akbar, "Differential Evolution Based Reliable Cooperative Spectrum Sensing in the Presence of Malicious Users", *Wireless Personal communication.*, Vol. 114, pp. 123-147, 2020.

[20] A. Guirguis, M. Karmoose, K. Habak, M. E. Nainay, and M. Youssef, "Cooperation-based multi-hop routing protocol for cognitive radio networks", *Journal of Network and Computer Applications*, Vol. 110, pp. 27-42, 2018.

[21] X. Tang, J. Zhou, S. Xiong, J. Wang, and K. Zhou, "Geographic Segmented Opportunistic Routing in Cognitive Radio Ad Hoc Networks Using Network Coding", *IEEE Access*, Vol. 6, pp. 62766-62783, 2018.

[22] N. Gul, S. Khan, S. Kim, J. Kim, and Z. Khalil, "Boosted Trees Algorithm as Reliable Spectrum Sensing Scheme in the Presence of Malicious Users", *Electronics*, Vol. 9, No. 1038, 2020

[23] Z. Luo, S. Lu and S. Yalin, "When Attackers Meet AI: Learning-empowered Attacks in Cooperative Spectrum Sensing", *IEEE Transactions on Mobile Computing*, Vol. 21, 2019.

[24] P. Venkatesan and J. Vijayarangan, "Secure and reliable routing in cognitive radio networks", *Wireless Networks*, Vol. 23, pp. 1689-1696, 2017.

[25] M. Zareei, M. Mohamed, H. Anisi, and K. Khan, "On-Demand Hybrid Routing for Cognitive Radio Ad-Hoc Network", *IEEE Access*, Vol. 4, pp. 8294-8302, 2016

[26] G. Ferraioli, B. Kanoun, V. Pascazio, and G. Schimzi, "SAR image restoration via a NL approach based on the KS Test", *In Proc of IEEE Int. Geosci. Remote Sens. Symp*, pp. 5820-5822, 2018.

[27] C. Cui, H. Man, Y. Wang, and S. Liu, "Optimal Cooperative Spectrum Aware Opportunistic Routing in Cognitive Radio Ad Hoc Networks", *Wireless Personal Communications*, Vol. 91, No. 1, pp. 101-118, 2016.

[28] T. Tran, V. Nguyen, K. Shim, and B. D. Costa, "A Deep Reinforcement Learning-Based QoS Routing Protocol Exploiting Cross-Layer Design in Cognitive Radio Mobile Ad Hoc Networks", *IEEE Transactions on Vehicular Technology*, Vol. 71, No. 12, 2022.

[29] D. Singhal and M. Garimella, "Cognitive cross-layer multipath probabilistic routing for cognitive networks", *Wireless Networks*, Vol. 21, No. 4, pp. 1181-1192, 2015.

[30] C. Jing, U. Junsheng, Y. Wenchao, and W. Shuochen, "Multi-metric cross layer routing protocol for cognitive radio ad hoc networks", *Journal of Xidian University*, Vol. 45, No. 2, pp. 77-83, 2018.

[31] Wang, Jihong, and C. Liu. "An imperfect spectrum sensing-based multi-hop clustering routing protocol for cognitive radio sensor networks", *Scientific Reports*, Vol. 13, No. 1 p. 4853, 2023.

[32] Q. Salih, M. Rahman, M. Arafatur, and T. Asyhari, "Dynamic channel estimation-aware routing protocol in mobile cognitive radio networks for smart IIoT applications", *Digital Communications and Networks*, Vol. 9, 2023.

[33] A. Khalid, H. Darabkh, and B. Salameh, "Efficient Routing Protocol for Optimal Route Selection in Cognitive Radio Networks Over IoT Environment", *Wireless Personal Communications*, Vol. 129, No. 1 pp. 209-253, 2023.

[34] Z. Zhang, S. Sun, M. Liu, Z. Li, and Q. Zhang, "Rendezvous Delay-Aware Multi-Hop Routing Protocol for Cognitive Radio Networks", In: *Proc. of International Conference on Mobility, Sensing and Networking (MSN)*, pp. 28-35, 2022.