electronics

MDPI

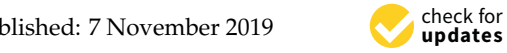
Article

A Trust Framework to Detect Malicious Nodes in Cognitive Radio Networks

Geetanjali Rathee [1], Farhan Ahmad [2,*], Chaker A. Kerrache [3] and Muhammad Ajmal Azad [2]

1 Department of Computer Science and Engineering, Jaypee University of Information Technology, Waknaghat, Solan 173234, India; geetanjali.rathee123@gmail.com
2 Cyber Security Research Group, College of Engineering and Technology, University of Derby, Derby DE22 3AW, UK; m.azad@derby.ac.uk
3 Department of Mathematics and Computer Science, University of Ghardaia, Ghardaia 47000, Algeria; ch.kerrache@univ-ghardaia.dz
* Correspondence: f.ahmad@derby.ac.uk

Received: 30 September 2019; Accepted: 4 November 2019; Published: 7 November 2019



Abstract: Cognitive radio is considered as a pioneering technique in the domain of wireless communication as it enables and permits the Cognitive Users (CU) to exploit the unused channels of the Primary Users (PU) for communication and networking. The CU nodes access the vacant bands/channels through the Cognitive Radio Network (CRN) cycle by executing its different phases, which are comprised of sensing, decision making, sharing (accessing) and hand-off (mobility). Among these phases, hand-off is the most critical phase as the CU needs to switch its current data transmissions to another available channel by recalling all the previous functions upon the emergence of a PU. Further, 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 such as the Cognitive User Emulation Attack (CUEA) and Primary User Emulation Attack (PUEA) may be encountered by the handoff procedure, which need to be resolved. To address this issue, a secure and trusted routing and handoff mechanism is proposed 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 Analyser (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). The simulation results suggest that the proposed solution leads to 88% efficiency in terms of better throughput of CRN during data communication, the packet loss ratio, the packet delivery ratio and the maximum and average authentication delay and clearly outperforms the prevailing mechanisms in all the parameters.

Keywords: trust analyser; trusted CU; social impact theory optimizer; handoff CU security; rating trust value; trusted network nodes

1. Introduction

New innovations in wireless technologies and enhancement in broadcasting services on multimedia platforms have not only resulted in a colossal increase in the demand and usage of the communication spectrum, but have also called attention to the immense problem of spectrum scarcity [1]. However, the statistics of spectrum usage in most countries have also exposed the problem

of spectrum under-utilization. Spectrum under-utilization is used to describe the bands/channels that have been allotted to licensed users, but cannot be efficiently utilized and remain vacant most of the time. Therefore, by taking advantage of this opportunity, a promising Cognitive Radio (CR) technology [2,3] (as depicted in Figure 1) has been pioneered in the field of wireless transmission, which enables the Cognitive Users (CUs) or unlicensed users to exploit the unused bands/channels of the Primary Users (PU)/licensed users. Spectrum sensing, decision making, sharing and mobility (handoff) are the potential functions performed by a CR via cognitive engines to occupy an idle spectrum band of the PU [4,5]. During the first three functions, the CU interacts with its environment to recognize idle bands and selects the most appropriate amongst all the bands sensed as idle. Next, it ascertains the transmission on the selected idle channel via a suitable accessing strategy in order to evade an obstruction of communication among the PUs and CUs [6,7]. However, during the mobility or handoff functioning of CR, the CU needs to switch its current data transmission on another available channel upon the emergence of PU by recalling all the previous functions [8,9]. The data transmission time, spectrum sensing time and appearance of PU are the key facets that increase the delay during the handoff process [10]. Further, from the security perspective, it is possible for an intruder or a malicious user (MU) to imitate a legitimate Handoff CU (HCU) with the intention to degrade the network performance [11].

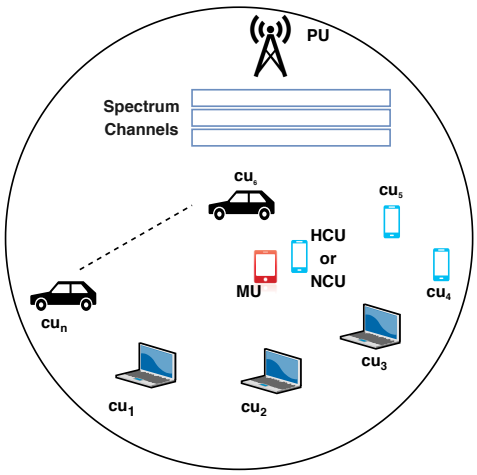


Figure 1. The CU (Cognitive Users) handoff mechanism for a cognitive radio network cell.

1.1. Motivation

In the conventional handoff techniques [12,13], all the CUs are often assumed to be cooperative and trusted. However, in practice, the HCUs or New Cognitive Users (NCUs) (where a new CU enters into a CR cell for the first time after the network establishment) can be conciliated by the MUs to introduce malicious activities in the Cognitive Radio Network Cell (CRNC) environment [14].

The motives of the MU are to prevent the legitimate CUs from accessing the channel by repetitively mimicking the serving PU's signal and damaging the network metrics and hand-off security in the environment. Another way to breach the CRN security is to compromise the intermediate nodes through which the CUs transmit their data. The wireless scenery and communication measures allow the data of a CU to be transmitted through various intermediate nodes. Hence, there might be a prospect where intermediate nodes may be compromised by an MU to perform malicious functions. The intruder may compromise one or more network devices such as hubs, bridges or routers so as to consume the system's resources. Further, where a large number of unknown objects communicate in a colossal sphere, there is forever a high prospect for MUs to gain illicit network admittance of the CUs. Therefore, the potential challenge of CRNC security is to transmit the data of CUs through trusted nodes and secure the HCU or NCU by ascertaining a trusted handoff framework. Till now, researchers have proposed various security frameworks for PU or CU transmission; however, only a few of

them have focused on the security aspects of handoff or intermediate data transmission. Therefore, until now, the CU's intermediate nodes and spectrum handoff security techniques are unexploited for the Cognitive Radio Network (CRN) in the reported literature. A number of cryptographic security/privacy frameworks have been proposed for data mobility or transmission of nodes in several environments such as MANETs, VANETs, UAVs, WMN and WSN [11,15–22]. However, these methods may not be directly espoused in the CRN milieu owing to its unique individuality. Further, the cryptographic proposals might increase the communication, storage and computation expenses by directly increasing the transmission delay.

Currently, the authenticity of the devices or applications can be deliberated through the trust value approach [23–27]. The network trust is distinct as a computing parameter that calculates the legality of a meticulous node based upon its previous or existing communications without increasing the cryptographic steps. Therefore, an efficient method to ensure a secure message system is a trust based process. It enhances the security without further increasing the network delay and overhead. Unluckily, trusted security frameworks/methods in CRN have not been methodically identified and are still in their early stages.

1.2. Contribution

The paramount objective of this paper is to propose a secure framework that effectively transmits the data of cognitive users through trusted nodes and legitimises the HCU or NCU, where the trust rate of each node and its neighbour is computed by initiating a Trust Analyser (TA) among the nodes and CUs. The goal of TA is to confirm the legitimacy of the transmitting node by calculating its rating and trust based on its previous history connections using SITO. This research study also seeks to search for a trusted path for communication using the Tidal Trust Algorithm (TTA). The potential contributions of the proposed framework are as follows:

1. Recognizing the role of the trust based security structure in the CRN milieu.
2. Recommending a trusted security structure for the CRN environment via the TTA algorithm by computing the TF (Trust Factor)/TV (Trust Value) of each node.
3. Ensuring a secure data transmission among CUs by computing their rates and trust values using SITO.

The remaining structure of the manuscript is organized as follows. The related survey of the secure CRN milieu is offered in Section 2. Further, a trusted security scheme for the communication of the Network Node (NN) and CU is given in Section 3. In addition, Section 4 examines the performance factors of the given framework in various scenarios. Further, the outcomes of exhaustive simulation results against various networking parameters are discussed in Section 5. Finally, Section 6 provides the conclusion and highlights the future directions of the work.

2. Related Work

Handoff is an essential function of CRN. This section deliberates the various handoff security techniques and frameworks of the CRN environment. Several researchers have described various handoff schemes by categorizing them into two major categories, i.e., (1) reactive handoff schemes and (2) proactive handoff schemes. Wang et al. [28] gave a reactive handoff procedure where the preemptive recommence precedence queuing system is used to exploit the channel accessibility under diverse service time distributions and traffic survival rates. Moreover, the network metrics are measured beside broadcast latency and traffic survival rates. However, the proposed framework fails to identify malicious nodes that remain ideal for a long period of time in the network and perform replay and man-in-the-middle attacks to affect the networking parameters. In order to overcome this issue, Wu et al. [29] gave a proactive scheme in which a common optimal communication with proactive spectrum handoff (OPTH) technique was applied along with dynamic programming to overcome the issue of data message communication in a predefined target. Further, the simulated results attained

total minimal costs and higher data rates in comparison to conventional techniques. In addition, Tayel et al. [30] presented an indiscriminate diagnostic model to minimize the data communication time for CU throughout the handoff. The simulation consequences were demonstrated based on the preemptive recommence precedence network. However, the authors did not discuss the energy transmission/consumption required by each node to process the communication mechanism in the network. In addition, none of the authors till now have introduced the need for security during the handoff mechanism. Liu et al. [31] proposed an energy efficient and secure mechanism using the secrecy guard zone in order to secure the primary transmitters. The authors gave a stochastic geometry random CRN for analysing the probability of primary links whose numerical and analytical results validated the proposed framework over conventional approaches. Further, Maji et al. [32] exploited the importance of physical layer security by evaluating a secrecy outage probability in terms of energy harvesting based upon underlay CRN. The proposed approach's aim is to determine eavesdropping during the direct link data transmission and analysed against the target data rate, energy harvesting time, interference threshold and secrecy rate. However, the amount of time required to ensure or validate the authenticity of users was missing in this specific study.

In addition, Shah et al. [33] proposed a physical layer secure framework for orthogonal frequency division multiplexing. The improved proposed framework was shown against different measuring parameters in terms of the secrecy rate. Zhang et al. [34] proposed a technique that takes minimum power consumption in two different schemes, namely the underlay scheme and cooperative scheme. In both schemes, the CU was non-trusted. Using an optimization tool, the authors designed a secure beam forming for both schemes. Further, the simulated results validated the proposed phenomenon against conventional approaches. However, they did not discuss the dynamic scenarios or the probability of intruders to forge the legitimate CU that start behaving as MU after remaining ideal for a longer time in the network. Salameh et al. [35] proposed a probabilistic channel assignment mechanism in order to overcome the jamming attack for both reactive and proactive approaches. The proposed mechanism minimizes the invalidity of packet transmission that averts delay constraints. The simulated results validated the proposed framework over availability, security and the quality-aware channel algorithm against a number of conventional approaches. However, the authors did not discuss the major security threats such as the amount of energy or network resources consumed during a worm hole threat. Moreover, Roshni et al. [36] proposed a technique in order to establish a raw energy level of the PU that is an h-hop distance away using non-consensus disseminated spectrum sensing. In addition, a data falsification attack was considered during the vacant spectrum selection. In order to distinguish the maliciously performing nodes, a secure node generation approach was used that isolated the node generating maximum energy values. The numerical and simulated results against legitimate node selection validated the proposed mechanism. Furthermore, the process to identify or validate the legitimate nodes in the network needed complex computational and communications overheads.

In addition, several authors have proposed security mechanisms based on trust computations in cognitive radio networks. Bennaceur et al. [37] surveyed the security mechanisms based on the trust and reputation mechanism. The authors illustrated the trust based mechanisms by categorizing them into basic, probability based, intelligent trusted mechanism and trust through the involvement of a third party. In addition, Jin et al. [38] proposed an approach for ensuring the trust among CU using the efficient energy mechanism where the user's trust is established through the node's opinion. The CUs having a legitimate or untrusted opinion of another node would be accepted by the entire network. Furthermore, Dubey et al. [39] and Sun et al. [40] proposed a trust based mechanisms in CRN based on distance and location awareness among the CUs through certain metrics such as Quality-of-Service (QoS) links and requirements. In addition, the probability based reputation mechanism was proposed to detect spectrum sensing falsification threats in the cooperative sensing approach.

Several researchers have proposed trusted and efficient security procedures for handoff techniques by exploring the delay parameter in CRN and the Primary User Emulation Attack (PUEA), where an

MU imitates the characteristics of a PU in order to stop the CUs from accessing the available channel. However, the security aspects during the spectrum handoff process are missing in the reported literature. In auxiliary, none of the researchers have considered the trust of intermediate nodes through which the CUs' data are transmitted. Upon the appearance of the PU transmitter, the HCU needs to vacate the occupied spectrum band and search for a new unused channel to resume its additional transmissions. Further, the prevention of other nodes from using the channels for communication by occupying them is a type of jamming attack that also degrades the networking process significantly. Therefore, ensuring a secure trust based routing mechanism from intermediate nodes is discussed in this paper. Now, In the spectrum handoff schemes, during the delay to occupy or vacate another unused channel, there may be the possibility of an MU behaving as a legitimate CU or PU with the intention of never allowing the HCU to occupy another channel or with the intention of simply degrading the network performance. This attacking strategy has pioneered a new security threat in handoff security, i.e., "Cognitive User Imitate Threat (CUIT)", where the MU never allows the HCU to access the new unused band by mimicking the legitimate CU. In the next section, we provide the details of our proposed framework.

3. CR Secure Handoff Mechanism

The architecture of the CRN environment is depicted in Figure 2, which is comprised of three distinct layers. (1) the primary user layer allows the PUs to access the reserved bands or channels of the network at any time; (2) the Network Node (NN) layer is responsible for transmitting the data of CUs; and (3) the CU layer allows the users to access the idle band of the PUs.

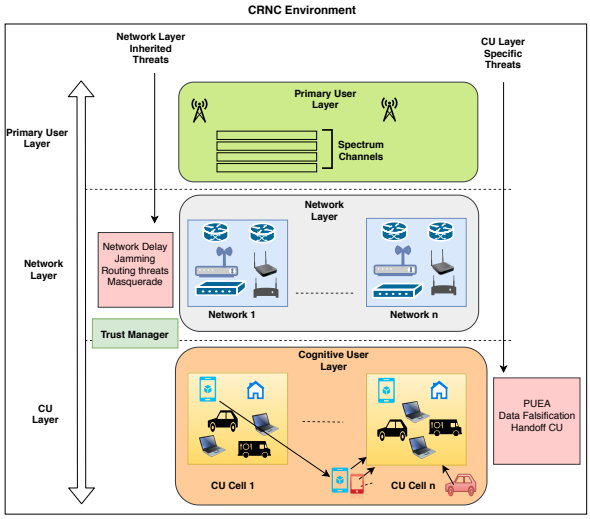


Figure 2. The Cognitive Radio Network Cell (CRNC) milieu together with specified and inherited security attacks. PUEA, Primary User Emulation Attack.

In the case where a CU wants to access an idle band, NN calculates the Trust Value (TV) of the requesting CUs by validating it with the predefined thresholds. If the CU's TV is greater than the NN rating, then the CU is trusted and permitted to access the band. A TA is maintained that keeps a record of all the parameters of the nodes in its look-up/routing table the including node's address (addr), id, rating and TF/TV. Therefore, the proposed framework identifies trust at two different levels, i.e., (1) during data transmission at the NN layer and (2) at the CU layer, where either NCU or HCU may get compromised. In the next section, we provide the details of the system model.

3.1. System Model

In addition, the trust of each NN layer is calculated using the Tidal Trust Algorithm (TTA), which generally works in two diverse phases: (1) During network establishment, all the nodes are assumed to be trusted in nature, where the ratings and trust of every individual node are computed as the nodes start the communication process in the network. The trust and rating of every node is computed by separating them into certain levels such as the trust of nodes at $i + 1$ will be calculated by nodes present at level i. (2) In the subsequent phase, NN calculates the trust of each HCU or NCU before allowing the data transmission through the trusted intermediate paths. The detailed explanation of the NN and CU layers is detailed below. Further, the flowchart of the proposed framework is depicted in Figure 3.

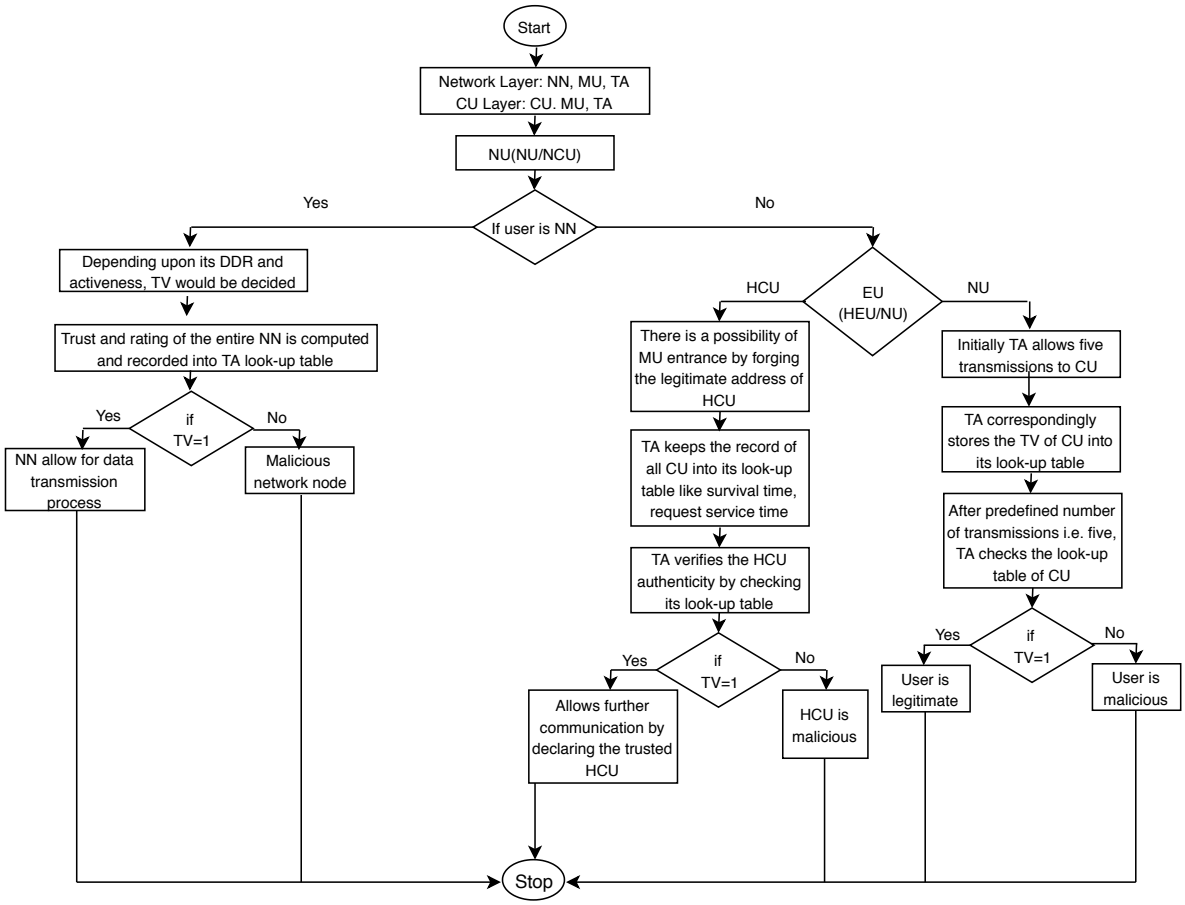


Figure 3. Proposed framework at the network Layer.

3.1.1. AT the NN Layer

To understand the operation of the proposed framework, we considered a unidirectional relationship between the nodes in the network. Upon starting the transmission process among nodes, the trust of every node is calculated through the SITO technique, which assigns a random trust to every node among 0–1. The ratings and trusts of all the nodes are subsequently updated and stored into the TA lookup table. As the communication proceeds, the primary part of TTA commences the processing by arbitrarily choosing the node for calculating the TV of its neighbouring nodes that are divided into certain levels. All network nodes are positioned at specific predefined levels, for instance the first node (P) at Level 0, Q, R, S at Level 1, etc., as illustrated in Figure 4a.

This procedure extends in a recursive way at each level for computing the neighbouring nodes' TV using their preceding history of communications. Figure 4a represents the graph state after the first flow of TTA, i.e., Level 0 values. For instance, in Figure 4a, node Q is rated as 0.35 because the trust

of node P for Q stands at 0.35 (depending upon their previous history interaction). Likewise, nodes R and S are rated as 0.30 and 0.40 respectively by node P. At Level 1, after each node has been rated, the TTA continues with subsequent steps till other nodes are rated. Each node at Level 1 will give an auxiliary rating to its respective neighbour at Level 2. If any node of Level 2 has more than one predecessor, then out of the assigned trust values, the minimum of the two would be considered due to the fact that no prior history of the node is available.

Figure 4b depicts the graph status subsequent to the algorithm where node T is rated by its predecessors R and Q. Node R rated T as 0.40, which is computed as such because it is the minimum of the trust value given by R to T, i.e., 0.40, and R's own rating of 0.50. Likewise, Q rated T as 0.35, which is the least of its rating of 0.35 and its trust over T, i.e., 0.45. The ultimate rating of T would be the highest between these two ratings, that is 0.40. In auxiliary, after accessing all the network nodes, the last node's rating, i.e., T's rating (0.40) (according to this network), would be selected as the threshold value of the network. The first half of algorithm runs in Breadth First Search (BFS) manner. Its goal is to vigorously ascertain the threshold of the trust between NN (source) and CU (destination). It is done upon the assignment of ratings to all other nodes in the last graph level that are assigned to CU. Now, if an NN is compromised as shown in Figure 4b, nodes R and U are compromised nodes, and the rating and TV of that node would probably be very less, which can be measured for further communications. The complete execution of the NN layer is presented in Algorithm 1. Furthermore, the algorithms of the involved functions to execute the main algorithm are highlighted in Algorithms 2–6, respectively.

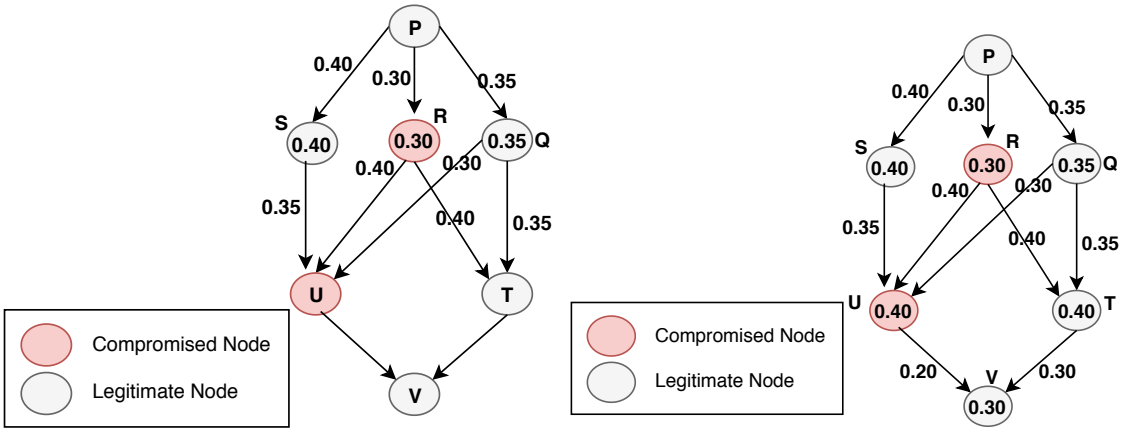


Figure 4. (**a**) Trust Value and rating at Level 1; (**b**) trust value and rating at Level 2.

Algorithm 1: Computation of the rating and TF/TV of all CNs.

Assumption: All the cognitive nodes are divided into certain levels (i.e., as depicted in Figure 5: node P is at Level 0, nodes Q, R and S are at level 1, and so on)
Input: A network with n number of cognitive nodes
Output: Node identified as either legitimate or malicious
Step 1: Primarily each node NN_i computes the TF/TV of its neighbouring nodes via SITO by calculating the following factors;
Compute activeness ();
Compute DDR();
Step 2: Apply TTA at every level so as to calculate or finalize the rating and trust of each NN_i
Compute level of trust ();
Compute rating ();
Step 3: At level i, NN_i dispenses the rating and TV to level $(i+1)$ NN_i
Step 4: Extinction of the recursion Step 3 waiting for all the NN_i to have the rating and TV

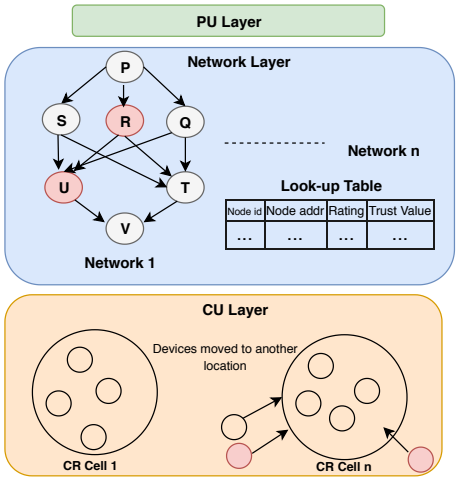


Figure 5. System model of the NN layer.

Algorithm 2: Calculation of Activeness().

Input: The number of transactions/communications done by each node is recorded to compute their TV/TF

Counter = 0

if *(NCU transmits desire (hello) message to CCU)* **then**

  Set Counter = counter + 1 ;

  if $(Counter > Counter_{threshold})$ **then**

    NCU is MU;

  else

    NCU is trusted CU

  end

else

  NCU is legitimate CU

end

Algorithm 3: Calculation of DDR().

Input: The amount of data transmitted among nodes

DDR = DDR($indegree_{packets}$-$outdegree_{packets}$) $\times$ 100

if $(DDR <= DDR_{thresholdvalue})$ **then**

  Set NCU as MU;

  return 1;

else

  Set NCU as trusted CU;

  return 0;

end

Algorithm 4: Calculation of TF().

Input: The number of communications done by each CU
if *(DDR and activeness > predefined threshold)* **then**
    Legitimate NN;
    return 1;
else
    Malevolent NN;
    return 0;
end

Algorithm 5: Calculation of Level Trust().

Input: The number of transactions/communications done by each IoT device is recorded to compute their TF
Primarily the NN_i at level i consigns the rating and TV to each CU_i
if *(at level i + 1, NN_i has more inputs from level i)* **then**
    TV depends on the TV and rating of level i;
else
    At level i + 1;
    Trust = Min (NN_i(TV), NN_i(rating));
    Max (TV (NN_1, NN_2..... NN_i));
end

Algorithm 6: Calculation of Rating().

Input: The TV and ratings of all CUs
1. At level i, NN_i consigns the TV that will rate the NN_i at level i + 1.
2. The level i + 1 rating will likely be
Rating = Max (level i (NN_i (rating)))

3.1.2. AT CU Layer

In subsequent algorithms of the given framework, trust towards the CU is calculated via the number of intermediate NNs. In this study, every NN in the graph computes its trust value for CU via Equation (1):

$$t_{n_i} = \frac{t_{n_{i,j}}, cu_i | t_{i,j} >= max}{t_{n_i}, j | t_{i,j} >= max} \quad (1)$$

where t_{n_i} is the threshold trust between nodes n_i and n_j at the network layer and CU_i and CU_j at the CU layer. Nodes that are legitimate and trusted will calculate the threshold trust towards the CU by Equation (1), which is the deciding parameter to strain out the nodes with the minimum trust ratings. Once trust values are calculated, only devices above threshold ratings are used to forward the messages. This is recursive for each node level, until the source is arrived at and its TV over the sink is computed. In that case, NN will compute the trust over HCU/NCU by the above process and derive the best available path to offer the communication. Moreover, communication between the devices is allowed only if the trust is above the threshold level. Algorithm 7 summarizes the execution process to calculate the legitimacy of CU.

Algorithm 7: Compute the best trusted path among NN_i and CU_i.

Input: Network with N_i number of nodes and CU_i of users
Output: Node identified as either legitimate or malicious
Step 1: CU_i communicates with NN_i.
Step 2: To ensure a trusted routing path, NN_i computes the threshold rating using the level of trust ()
Step 3: NN_i computes the multiple routes to CU_i by contrasting each NN_i (rating value) amid the threshold rating
Step 4: **if** *(NN_i rating > threshold rating)* **then**
  Embrace that node NN_i is in the route;
else
  Remove that node from the route
end
Step 5: NN_i will calculate the preeminent trusted route via Equation (1)

4. Performance Evaluation and Complexity of the Proposed Approach

Even though it is very difficult to ensure a secure routing and communication process at the network and cognitive layer, in this paper, we propose a trusted communication structure that not only offers high trust among the nodes, but also provides affordable genuine services to the CU. Figure 6 shows the abstracted scrutiny of the test bed with three cognitive networks operating on NS2 with a predefined number of CUs. Tables 1 and 2 present the CRN milieus of 500 m × 500 m having different numbers of nodes. In addition, the proposed phenomenon was validated against malevolent scenarios where a number of legitimate nodes were compromised by the intruders.

The CUs were movable in nature, where they could escape from their network or unite at any time. The mobility rate of CU was fixed at 0–10 m/s with the communication range of 30 m. Furthermore, the underlying MAC layer protocol was 802.11, while the communication range of the routers was set to 120 m. The preliminary random TV was also allocated to every node. Primarily, 250 CUs were formed, which operated as IoT devices. In addition, an artificial data creator was used that generated the data through normal delivery pattern. So as to compute the security, the malevolent nodes or CUs were embedded into the environment using the probability distribution during the handoff and communication process.

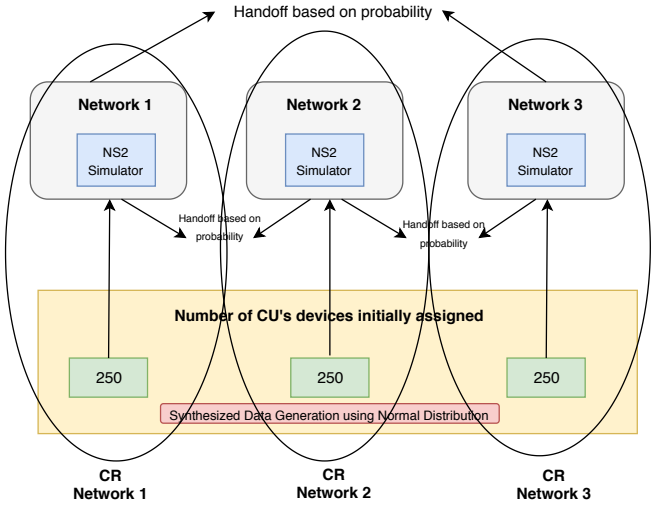


Figure 6. Testbed for the performance scrutiny of the proposed structure.

Table 1. Simulation parameters.

Parameters	Values
Simulation Time	80 s
Grid Facet	500 m × 500 m
CRN Nodes	250
Transmission Range	140 m (approximately)
Data Size	512 bytes
MAC Protocol	IEEE 802.11

Table 2. Arrangement of NS2 for the diverse CRN milieu.

Virtual Machine	Nodes	Edge Nodes (Near the CRN Environment)
CRN1	50	10
CRN2	100	15
CRN3	250	20

The black hole and worm hole are considered as severe routing attacks, as the former drastically affects the network metrics by dropping 100 percent of the data packets, while the latter selectively drops the data and cannot be recognized quickly [41]. The handoff occurs when any IoT device switches from one CRN to another upon the emergence of a PU. The involvement of HCU and malevolent CU and the alteration of CU to malevolent in the network are based on probability, as shown in Table 3. In addition, the conversion of the trusted node to malevolent through the handoff process states that among 100 handoffs, 10 nodes are converted to malicious. Initially, 50 nodes are dispensed to each CRN, and after every 80 s, more nodes are allotted in order to test the structure scalability.

Table 3. Dissimilar probabilities for the performance scrutiny of the given structure.

S.No.	Action	Probability
1	Accumulation of Malevolent Node	15
2	Handoff Nodes	10
3	Conversion to Malicious during Handoff	10

The architecture of our framework consisted of a TA, responsible for authenticating the legality of CU and HCU, and two gateway routers that ensured connectivity between the routers and the Internet. NN were divided into diverse zones that offered the services to their domains or zonal CU's as Home Routers (HR). The realms were assembled based upon the transmission variety of CU with its HR.

5. Simulation Results

In this section, we evaluate our proposal against the existing baseline model based on various performance evaluation metrics and criteria.

5.1. Performance Evaluation Metrics

In order to evaluate the performance of the proposed mechanism, we considered the following evaluation criteria, including:

1. Relative Trust: This metric is related to the trust of the network, indicating the highly trusted parameter in order to ensure a node's legitimacy. It is calculated via Equation (2):

$$RT = \sum_{i=1}^{N} (PDR_i + RE_i + ND_i + AS_i + PL_i \; and \; PHI_i) \quad (2)$$

2. Packet Delivery Ratio (PDR): This depicts the amount of packets that are successfully received by the nodes. Let P_R be the number of received packets and P_{exp} the number of packets that are expected to be received in the network.

$$PDR = \frac{P_R}{P_{exp}} \tag{3}$$

3. Packet Delivery Delay (PDD): This shows the amount of delay required by each (legitimate/malicious) node to forward the incoming packets. Let PRT be the total number of packet received and PGT the total number of packets generated, then PDD can mathematically be represented as:

$$PDD = PRT - PGT \tag{4}$$

4. Network throughput: This is defined as the total number of packets transmitted by the source node over the number of packets received by the destination node at a given period of time. Let T_{tp} be the total number of packets transmitted and T_{rp} the total number of packets received, then the network throughput can be given as:

$$NetworkThroughput = \sum_{i=1}^{N} \frac{Total\ number\ of\ packets}{T_{tp} - T_{rp}} \tag{5}$$

5. Average Authentication Delay (AAD): This is defined as the average amount of time required for validating the number of nodes. AAD is a request delay that indicates the difference between the time taken by requesting nodes and the time to authenticate it.

$$AAD = \sum_{i=1}^{N} \frac{Time_{Rqst} - Time_{auth}}{Total\ number\ of\ requesting\ nodes} \tag{6}$$

6. Maximum Authentication Delay (MAD): This is the maximum time required to authenticate a particular node in the network.
7. True Positive Rate (TPR): This is defined as the measure of how efficiently the mechanism can identify the malicious number of packets as presented in Equation (7):

$$TPR = \frac{TP}{TP + FN} \tag{7}$$

where a True Positive (TP) is the number of packets that have been dropped after their successfully identification and registration as malicious by the network. In addition, a False Negative (FN) is the number of packets that have been forwarded instead of being dropped after their incorrect identification as benign.

8. True Negative Rate (TNR): TNR is the measure of the number of legitimate packets identified by the mechanism, as depicted in Equation (8):

$$TNR = \frac{TN}{TN + FP} \tag{8}$$

where a True Negative (TN) is the number of packets that have been forwarded after their correct identification as benign by the network. Further, a False Positive (FP) is the number of packets that have been dropped instead of being forwarded after their incorrect registration as malicious.

5.2. Existing Method

We compared the efficiency of our proposal against [24], where the probabilistic scenario of the false presence of PUEA is presented in the CRN environment. Further, this study also proposes an

attack-aware cooperative sensing mechanism that identifies the possibility of false PUEA during the transmission process. We evaluated the comparison of this study based on the performance evaluation criteria, mentioned above.

5.3. Results

We considered various parameters to compare our proposal against the existing mechanism. In traditional (existing) approaches, malevolent devices are not sensed based on TV; thus, the overall computational overhead and the complexities of managing cryptographic keys increase. However, in our proposed mechanism, throughput, PDR and authentication processes performed better, as the malicious devices upon detection were immediately removed from the network. Figure 7 illustrates the relative normalized weights of various parameters evaluating the trust of a particular node. In order to do so, we considered various parameters such as Residual Energy (RE), Node Delay (ND), Packet Loss (PL), Previous History Interaction (PHI), Trust Value (TV) and the ticket and Authentication Server (AS). As depicted in Figure 7, PL and TV had maximum relative normalized weights in comparison to the other parameters, thus ensuring that these were the most significant parameters to measure or identify the legitimacy of nodes. In addition, the RE transmitted by the nodes during communication had the least significance to compute the security. Further, in order to measure the legitimate or malicious nodes in the network, the authors analysed the relative trust parameter where the trust value was dependent on various factors such as the residual energy, previous history interaction, node distance and third party server (authentication server). The relative metric is related to the trust computation of the network, indicating the highly trusted parameter. Furthermore, in this section, a relative trust value as depicted in Figure 8a,b is analysed among the existing and proposed approach, where malicious devices were increasing at a rate of 10%. The legitimate or malicious node identification was entirely dependent on the computed relative trust. The node having a higher trust value depending on the previous history interaction, residual energy, node distance, etc., would be considered as a highly trusted or legitimate node. However, the node having low trusted value was considered as a malicious node and would never be considered in the communication process.

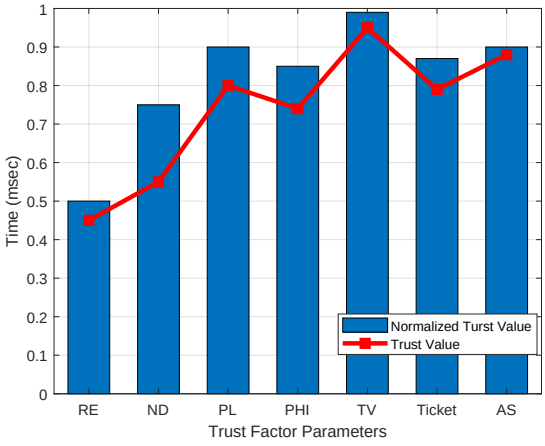
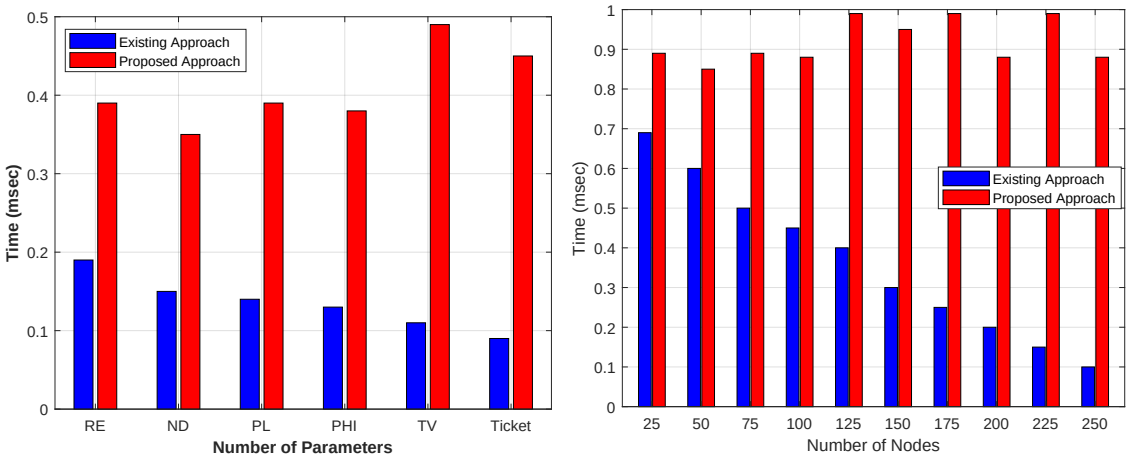


Figure 7. Relative normalized weights of the TV parameters for the handoff routing process.

Moreover, to identify MN from the network associated with a particular CU, we evaluated the accuracy of the proposed system in Figure 8a, where the comparison of the existing and proposed approaches is depicted. To measure the attacks, RE, ND, PL, PHI, TV and tickets were the certain factors that affected the network security while identifying the legitimacy of the node. However, for existing solutions, security was measured by analysing the probability of attacks during the communication process. Figure 8b depicts the ability of every node to compute trust when MDs were increased in the network. This suggests that trust computation by TA was varying by a small rate, while in the case of existing mechanisms (without involvement of the trust parameter), the time reduced as the

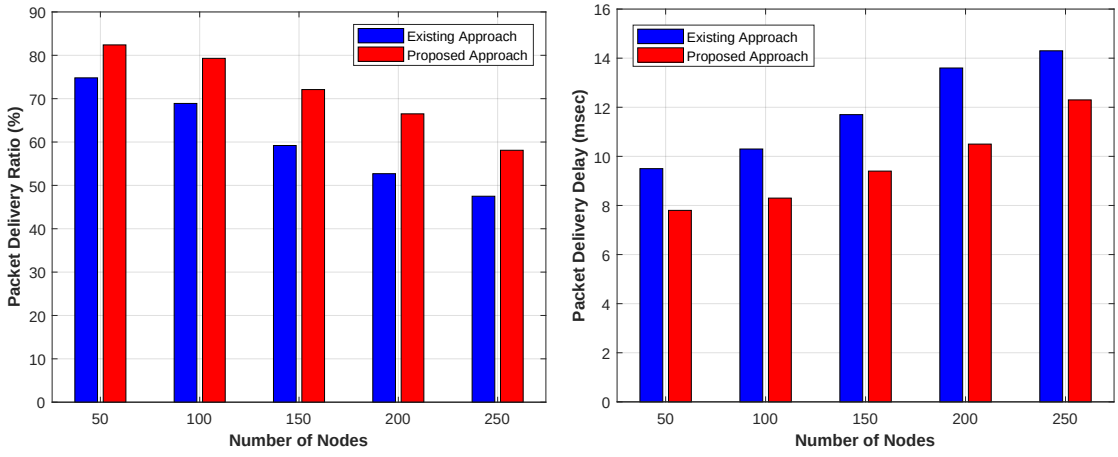
malicious number of nodes became involved in the transmission process. This was due to the fact that the involvement of malicious devices during the communication mechanism may significantly increase the packet transmission.



(**a**) (**b**)

Figure 8. (**a**) Relative trust evaluated by both approaches. (**b**) Trust evaluated by the nodes on different network sizes where the malicious nodes are increasing at 10 percent in every network size.

Additionally, Figure 9a,b represents the packet delivery ratio and packet delivery delay against the existing and proposed approaches. As is clearly seen in Figure 9a, our proposal achieved high PDR due to the fact that only trusted nodes were involved and participated in the routing process, while in the existing approach, the probability was identified to detect the malicious node that sometimes led to severe security concerns. Moreover, Figure 9b suggests that the proposed solution never was involved with the malicious nodes during the formation of the routing path. Therefore, the involvement of legitimate nodes increased the delivery rate between the source and destination. On the other hand, malicious nodes may get involved in the path formation process in the existing mechanism, which further increased the delay of the transmission process by generating Denial of Service (DoS) and replay attacks.



(**a**) (**b**)

Figure 9. (**a**) Packet delivery ratio. (**b**) Packet delivery delay (in time).

In addition, Figure 10 depicts the comparison of network throughput. In case the number of malicious nodes was fixed or less with the increase in network size, the existing approaches performed equivalent to the proposed mechanism. However, due to restriction in the involvement of nodes (only

legitimate nodes), the proposed approach still performed better. Finally, Figure 11a,b represents the packet delay in a scenario, where worm hole and black hole nodes were introduced to the network with 25 nodes. This clearly suggests that the delay caused by our proposed approach was less compared to the existing solution due to the fact that our solution never involved MD during the handoff or communication process, thus resulting in lower delays in the network. However, the existing approach may integrate MD within its communication, which ultimately allowed these nodes to degrade the network performance. Moreover, our proposed framework showed approximately an 88% success rate in packet delivery, throughput and trust computation against the existing mechanism.

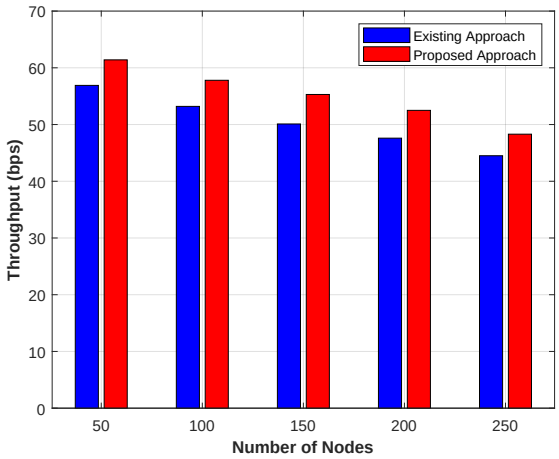
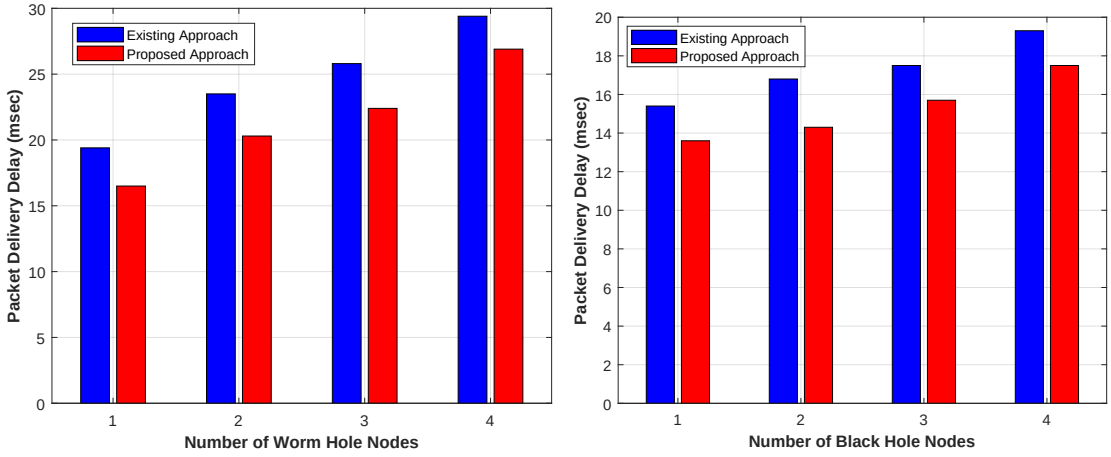


Figure 10. Network throughput.



(**a**) (**b**)

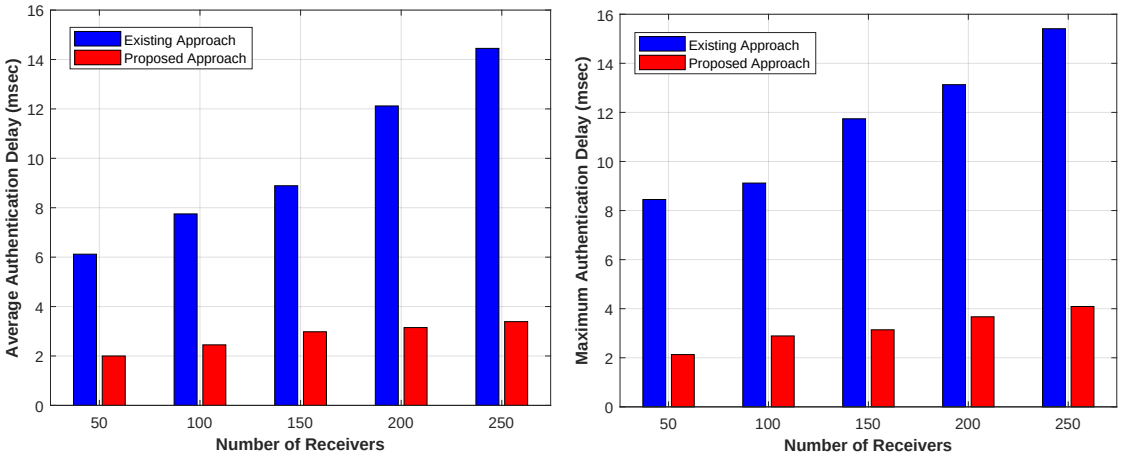
Figure 11. Packet delivery delay upon (**a**) increasing the number of worm hole nodes and (**b**) increasing the number of black hole node.

Finally, Figure 12a,b portrays the CU nodes' average and maximum authentication delay via TV and PHI examined by TA, suggesting that AAD and MAD of the proposed mechanism outperformed the existing approach. This was due to the fact TA validated the legitimacy of every node before allowing the transmission process. However, in the existing mechanism, malicious nodes may get involved in the communication process, which again led to the increase in the delay in the network.

To analyse the accuracy, the proposed mechanism was measured against average and maximum authentication delay. Further, the proposed approach was verified by identifying the malicious and legitimate behaviour of nodes against true the Positive Rate (TPR), also called the sensitivity, and the True Negative Rate (TNR), also called the specificity [42]. Figure 13a presents the specificity

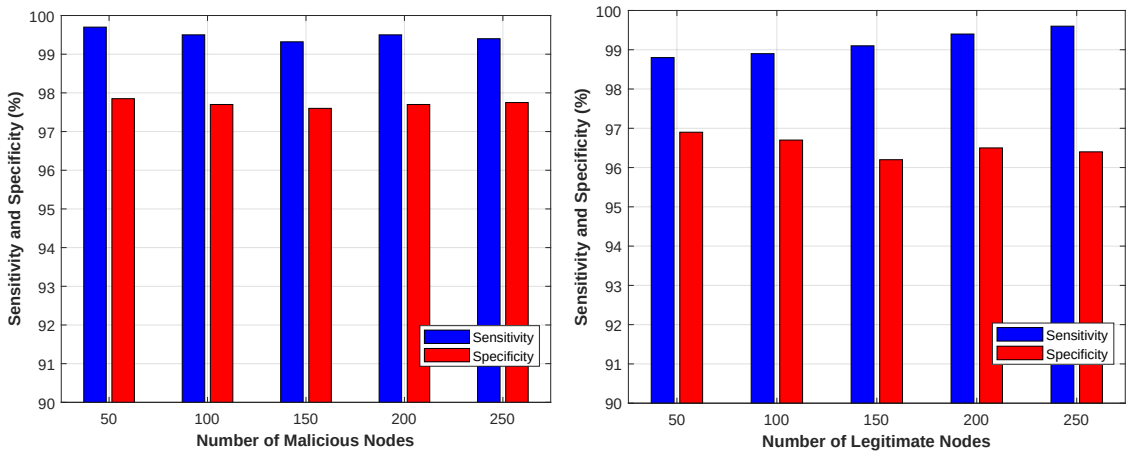
and sensitivity over various numbers of malicious nodes, whereas Figure 13b depicts specificity and sensitivity over various numbers of legitimate nodes.

The specificity and sensitivity of the proposed approach as depicted in Figure 13a were around 99% and 97%. respectively, over varying numbers of malicious nodes. The reason is that the trust analyser identified the trust rate of communicating nodes already present in the network immediately. The malicious behaviour of a node can also remain under surveillance by the TA for some specific period of time. However, the slightly smaller value in the case of specificity was because the newly-entered node remained unidentified and may have performed malicious activity in the network without coming into consideration for some time. Similarly, Figure 13b represents the 98% sensitivity and 96% specificity of the proposed mechanism against varying the number of legitimate nodes where TA validated the legitimacy of each communicating node present in the network before permitting to be involved in the transmission process.



(**a**) (**b**)

Figure 12. (**a**) Average authentication delay against the number of users (receivers). (**b**) Maximum authentication delay against the number of users (receivers).



(**a**) (**b**)

Figure 13. Sensitivity and specificity against (**a**) malicious nodes and (**b**) legitimate nodes.

5.4. Discussion

The proposed structure was evaluated on multiple NNs and CUs for which a modified test bed was given. The numerical experimentation evaluation was successful where numerous results concerning various metrics were evidenced. The system acted as desired, and all performance metrics were positive for the projected system for some CRN. The accuracy was nearly 88%, which can be

further recovered with time, due to the removal of identified MNs from the network. Additionally, the identification of MNs via the removal and trust of sensed MNs did not hamper the performance of the nodes. The projected system calculated the rating and trust of the nodes subsequent to a precise time interval. The nodes that negotiated and behaved malevolently would have low trust and rating (high PDR, low throughput, etc.) and would never be used for path formation. Likewise, TA computed the TV of the NCU or HCU before allowing the transmission process, which again increased the security aspect.

6. Conclusions

This paper initiated the concept of cognitive user attacks that occur during the spectrum handoff mechanism in cognitive radio networks. A trust analyser at the cognitive user layer successfully resolved CUEA by exploiting the behavioural characteristics of each CU using SITO. The proposed mechanism was validated extensively against conventional mechanisms by comparing various trusted and networking parameters. Furthermore, the proposed mechanism significantly outperformed the existing approaches by computing the trust of every CU or transmitting node. In addition, The TA ensured a trusted path for data transmission using TTA. The proposed framework showed an 88% success rate in all the simulation results against the existing mechanism.

The exploitation of the proposed framework for the inter-domain handoff communication is an exigent task that will be addressed in future communications.

Author Contributions: In this paper, all the authors contributed equally. The need for the trusted framework in cognitive radio networks during handoff along with the literature survey was done by G.R. and F.A. A secure framework for the handoff and routing mechanism using the trust analyser was addressed by G.R. and C.A.K. Further, the validation of the proposed mechanism based on various security criteria, such as the throughput of CRN during data communication, packet loss ratio, packet delivery ratio and maximum and average authentication delay and clearly outperforming the prevailing mechanisms in all the parameters, was detailed by F.A. The results' validation against existing mechanisms along with the success rate was analysed by M.A.A.

Funding: This research received no external funding.

Conflicts of Interest: The authors declare no conflict of interest.

Abbreviations

The following abbreviations are used in this manuscript:

CU	Cognitive User
PU	Primary User
CRN	Cognitive Radio Network
CUEA	Cognitive User Emulation Attack
HCU	Handoff Cognitive User
TA	Trust Analyser
SITO	Social Impact Theory Optimizer
NCU	New Cognitive User
TTA	Tidal Trust Algorithm
TF/TV	Trust Factor/Trust Value
OTPH	Optimal Transmission Proactive Spectrum Handoff
NN	Network Node
RE	Residual Energy
ND	Node Distance
PL	Packet Loss
PHI	Previous History Interaction
TPR	True Positive Rate
TNR	True Negative Rate
TP	True Positive
TN	True Negative

FP False Positive
FN False Negative

References

1. Mitola, J.; Maguire, G.Q. Cognitive Radio: Making Software Radios More Personal. *IEEE Pers. Commun.* **1999**, *6*, 13–18. [CrossRef]
2. Lee, W. Resource Allocation for Multi-Channel Underlay Cognitive Radio Network based on Deep Neural Network. *IEEE Commun. Lett.* **2018**, *22*, 1942–1945. [CrossRef]
3. Zheng, M.; Wang, C.; Du, M.; Chen, L.; Liang, W.; Yu, H. A Short Preamble Cognitive MAC Protocol in Cognitive Radio Sensor Networks. *IEEE Sens. J.* **2019**, *19*, 6530–6538. [CrossRef]
4. Li, S.; Xiao, S.; Zhang, M.; Zhang, X. Power Saving and Improving the Throughput of Spectrum Sharing in Wideband Cognitive Radio Networks. *J. Commun. Netw.* **2015**, *17*, 394–405. [CrossRef]
5. Ding, X.; Zou, Y.; Zhang, G.; Chen, X.; Wang, X.; Hanzo, L. The Security-Reliability Tradeoff of Multiuser Scheduling Aided Energy Harvesting Cognitive Radio Networks. *IEEE Trans. Commun.* **2019**. [CrossRef]
6. Mishra, M.K.; Trivedi, A.; Pattanaik, K. Outage and Energy Efficiency Analysis for Cognitive based Heterogeneous Cellular Networks. *Wirel. Netw.* **2018**, *24*, 847–865. [CrossRef]
7. Kumar, K.; Prakash, A.; Tripathi, R. A Spectrum Handoff Scheme for Optimal Network selection in Cognitive Radio Vehicular Networks: A Game Theoretic Auction Theory Approach. *Phys. Commun.* **2017**, *24*, 19–33. [CrossRef]
8. Piran, M.J.; Tran, N.H.; Suh, D.Y.; Song, J.B.; Hong, C.S.; Han, Z. QoE-Driven Channel Allocation and Handoff Management for Seamless Multimedia in Cognitive 5G Cellular Networks. *IEEE Trans. Veh. Technol.* **2016**, *66*, 6569–6585. [CrossRef]
9. Lu, H.; Zhang, L.; Jiang, M.; Wu, Z. High-Security Chaotic Cognitive Radio System with Subcarrier Shifting. *IEEE Commun. Lett.* **2015**, *19*, 1726–1729. [CrossRef]
10. Chae, C.J.; Cho, H.J. Enhanced Secure Device Authentication Algorithm in P2P-based Smart Farm System. *Peer Netw. Appl.* **2018**, *11*, 1230–1239. [CrossRef]
11. Fan, K.; Wang, J.; Wang, X.; Li, H.; Yang, Y. Secure, Efficient and Revocable Data Sharing Scheme for Vehicular Fogs. *Peer Netw. Appl.* **2018**, *11*, 766–777. [CrossRef]
12. Polese, M.; Giordani, M.; Mezzavilla, M.; Rangan, S.; Zorzi, M. Improved Handover through Dual Connectivity in 5G MMWave Mobile Networks. *IEEE J. Sel. Areas Commun.* **2017**, *35*, 2069–2084. [CrossRef]
13. Wang, L.C.; Wang, C.W.; Chang, C.J. Modeling and Analysis for Spectrum Handoffs in Cognitive Radio Networks. *IEEE Trans. Mob. Comput.* **2011**, *11*, 1499–1513. [CrossRef]
14. Nejatian, S.; Syed-Yusof, S.K.; Latiff, N.M.A.; Asadpour, V.; Hosseini, H. Proactive Integrated Handoff Management in Cognitive Radio Mobile Ad-Hoc Networks. *EURASIP J. Wirel. Commun. Netw.* **2013**, *2013*, 224. [CrossRef]
15. Akilarasu, G.; Shalinie, S.M. Wormhole-Free Routing and DoS Attack Defense in Wireless Mesh Networks. *Wirel. Netw.* **2017**, *23*, 1709–1718. [CrossRef]
16. Barka, E.; Kerrache, C.A.; Benkraouda, H.; Shuaib, K.; Ahmad, F.; Kurugollu, F. Towards A Trusted Unmanned Aerial System using Blockchain (BUAS) for the Protection of Critical Infrastructure. *Wiley Trans. Emerg. Telecommun. Technol.* **2019**. [CrossRef]
17. Rathee, G.; Saini, H.; Singh, G. Aspects of Trusted Routing Communication in Smart Networks. *Wirel. Pers. Commun.* **2018**, *98*, 2367–2387. [CrossRef]
18. Wu, F.; Xu, L.; Kumari, S.; Li, X. A New and Secure Authentication Scheme for Wireless Sensor Networks with Formal Proof. *Peer Netw. Appl.* **2017**, *10*, 16–30. [CrossRef]
19. Ahmad, F.; Franqueira, V.N.L.; Adnane, A. TEAM: A Trust Evaluation and Management Framework in Context-Enabled Vehicular Ad-Hoc Networks. *IEEE Access* **2018**, *6*, 28643–28660. [CrossRef]
20. Sultana, S.; Ghinita, G.; Bertino, E.; Shehab, M. A Lightweight Secure Scheme for Detecting Provenance Forgery and Packet Drop attacks in Wireless Sensor Networks. *IEEE Trans. Dependable Secur. Comput.* **2013**, *12*, 256–269. [CrossRef]
21. Altisen, K.; Devismes, S.; Jamet, R.; Lafourcade, P. SR3: Secure Resilient Reputation-Based Routing. *Wirel. Netw.* **2017**, *23*, 2111–2133. [CrossRef]

22. Ferng, H.W.; Khoa, N.M. On Security of Wireless Sensor Networks: A Data Authentication Protocol using Digital Signature. *Wirel. Netw.* **2017**, *23*, 1113–1131. [CrossRef]
23. Borkar, G.M.; Mahajan, A. A Secure and Trust based On-Demand Multipath Routing Scheme for Self-Organized Mobile Ad-Hoc Networks. *Wirel. Netw.* **2017**, *23*, 2455–2472. [CrossRef]
24. Sharifi, M.; Sharifi, A.A.; Niya, M.J.M. Cooperative Spectrum Sensing in the Presence of Primary User Emulation Attack in Cognitive Radio Network: Multi-Level Hypotheses Test Approach. *Wirel. Netw.* **2018**, *24*, 61–68. [CrossRef]
25. Zhu, C.; Rodrigues, J.J.; Leung, V.C.; Shu, L.; Yang, L.T. Trust-Based Communication for the Industrial Internet-of-Things. *IEEE Commun. Mag.* **2018**, *56*, 16–22. [CrossRef]
26. Gilbert, E.P.K.; Kaliaperumal, B.; Rajsingh, E.B.; Lydia, M. Trust based Data Prediction, Aggregation and Reconstruction using Compressed Sensing for Clustered Wireless Sensor Networks. *Comput. Electr. Eng.* **2018**, *72*, 894–909. [CrossRef]
27. Xu, D.; Zhang, S.; Chen, J.; Ma, M. A Provably Secure Anonymous Mutual Authentication Scheme with Key Agreement for SIP using ECC. *Peer Netw. Appl.* **2018**, *11*, 837–847. [CrossRef]
28. Wang, C.W.; Wang, L.C. Analysis of Reactive Spectrum Handoff in Cognitive Radio Networks. *IEEE J. Sel. Areas Commun.* **2012**, *30*, 2016–2028. [CrossRef]
29. Wu, Y.; Yang, Q.; Liu, X.; Kwak, K.S. Delay-Constrained Optimal Transmission with Proactive Spectrum Handoff in Cognitive Radio Networks. *IEEE Trans. Commun.* **2016**, *64*, 2767–2779. [CrossRef]
30. Tayel, A.F.; Rabia, S.I.; Abouelseoud, Y. An Optimized Hybrid Approach for Spectrum Handoff in Cognitive Radio Networks with Non-Identical Channels. *IEEE Trans. Commun.* **2016**, *64*, 4487–4496. [CrossRef]
31. Liu, X.; Zheng, K.; Liu, X.Y.; Wang, X.; Dai, G. Towards Secure and Energy-Efficient CRNs via Embracing Interference: A Stochastic Geometry Approach. *IEEE Access* **2018**, *6*, 36757–36770. [CrossRef]
32. Maji, P.; Roy, S.D.; Kundu, S. Physical Layer Security in Cognitive Radio Network with Energy Harvesting Relay and Jamming in the Presence of Direct Link. *IET Commun.* **2018**, *12*, 1389–1395. [CrossRef]
33. Shah, H.A.; Koo, I. A Novel Physical Layer Security Scheme in OFDM-based Cognitive Radio Networks. *IEEE Access* **2018**, *6*, 29486–29498. [CrossRef]
34. Zhang, M.; Liu, Y. Secure Beamforming for Untrusted MISO Cognitive Radio Networks. *IEEE Trans. Wirel. Commun.* **2018**, *17*, 4861–4872. [CrossRef]
35. Salameh, H.A.B.; Almajali, S.; Ayyash, M.; Elgala, H. Spectrum Assignment in Cognitive Radio Networks for Internet-of-Things Delay-Sensitive Applications under Jamming Attacks. *IEEE Internet Things J.* **2018**, *5*, 1904–1913. [CrossRef]
36. Rajkumari, R.; Marchang, N. Secure Non-Consensus based Spectrum Sensing in Non-Centralized Cognitive Radio Networks. *IEEE Sens. J.* **2018**, *18*, 3883–3890. [CrossRef]
37. Bennaceur, J.; Idoudi, H.; Azouz Saidane, L. Trust Management in Cognitive Radio Networks: A Survey. *Int. J. Netw. Manag.* **2018**, *28*, e1999. [CrossRef]
38. Jin, F.; Varadharajan, V.; Tupakula, U. A Trust Model based Energy Detection for Cognitive Radio Networks. In Proceedings of the Australasian Computer Science Week Multiconference, Brisbane, Autralia, 30 January–2 February 2017; p. 68.
39. Dubey, R.; Sharma, S.; Chouhan, L. Secure and Trusted Algorithm for Cognitive Radio Network. In Proceedings of the 2012 Ninth International Conference on Wireless and Optical Communications Networks (WOCN), Indore, India, 12 November 2012; pp. 1–7.
40. Sun, Z.; Xu, Z.; Chen, Z.; Ning, X.; Guo, L. Reputation-Based Spectrum Sensing Strategy Selection in Cognitive Radio Ad Hoc Networks. *Sensors* **2018**, *18*, 4377. [CrossRef]
41. Ahmad, F.; Adnane, A.; Franqueira, V.; Kurugollu, F.; Liu, L. Man-In-The-Middle Attacks in Vehicular Ad-Hoc Networks: Evaluating the Impact of Attackers' Strategies. *Sensors* **2018**, *18*, 4040. [CrossRef]
42. Kralevska, K.; Garau, M.; Førland, M.; Gligoroski, D. Towards 5G Intrusion Detection Scenarios with OMNeT++. 6th OMNet++ Community Summit, Hamburg, 2019. Available online: https://summit.omnetpp.org/2019/assets/pdf/OMNeT_Summit_2019_paper_1.pdf (accessed on 16 October 2019).