IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received August 11, 2020, accepted September 12, 2020, date of publication September 18, 2020,
date of current version September 30, 2020.

*Digital Object Identifier 10.1109/ACCESS.2020.3024662*

# Towards Securing Routing Based on Nodes Behavior During Spectrum Sensing in Cognitive Radio Networks

**MAHMOUD KHASAWNEH[1], (Member, IEEE), AHMAD AZAB[1], (Member, IEEE), AND ANJALI AGARWAL[2], (Senior Member, IEEE)**
[1]College of Engineering and Technology, American University of the Middle East, Kuwait
[2]Electrical and Computer Engineering Department, Concordia University, Montréal, QC H3G 1M8, Canada

Corresponding author: Mahmoud Khasawneh (mahmoud.khasawneh@aum.edu.kw)

This work was supported in part by the Research Fund of American University of the Middle East in Kuwait.

**ABSTRACT** Routing is a challenge in cognitive radio networks (CRNs) due to the properties of cognitive radio (CR) technology, as well as other limitations. Firstly, the CR's frequency band is considered a dynamic spectrum. Therefore, since the routing algorithms used in other types of networks rely on a fixed frequency band, they cannot be directly used in CRNs. Secondly, the dynamic spectrum access, which is enabled by CR technology, negatively affects the network performance. Thirdly, having an effective routing in CRNs needs a local and continual knowledge of its changeable environment. Lastly, the presence of adversary nodes and their malicious activities affect the route establishment process, thereby reducing the network performance. This paper addresses these limitations by combining the spectrum sensing and the spectrum management phases by proposing a novel and secure routing algorithm. Security in the proposed algorithm combines two aspects. The first aspect is measuring the nodes' behavior during the spectrum sensing phase through a parameter called belief level (BL), which refers to the nodes' reliability to correctly find and use the white spectrum channels. The second aspect is securing the routing request and reply messages by encoding them with the existing cryptography techniques. The main goal of the proposed approach is to make the available paths between any two communicating nodes secure, reduce the negative effects to the licensed users over the spectrum channels, and moderate the total cost of the used channels over the best path(s). The performance evaluation in terms of end-to-end delay, packet delivery ratio, packet loss ratio, and routing overhead show that the proposed approach outperforms multiple existing routing algorithms. Moreover, the proposed algorithm is validated and verified in terms of security functionality against any attacks.

**INDEX TERMS** Belief level, CRNs, routing, security, spectrum sensing.

## I. INTRODUCTION

In this era of 5G and IoT, cognitive radio (CR) technology is being considered one of the emerging technologies that enables open spectrum sharing for 5G. This promising technology can satisfy the strict spectrum requirement of 5G networks. CR is reconfigurable and adjustable which make it suit different environment characteristics [1]. In cognitive radio networks (CRNs), two types of users exist: unlicensed users, referred to as secondary users (SUs), and licensed users, referred to as primary users (PUs). The SUs can access the PUs spectrum channels when the PUs are inactive [1], [2].

As mentioned in [3], [4], physical and data link layers' issues, mainly spectrum sensing and interference avoidance, are the current main areas of research about cognitive radio. Finding the best path(s) between any two nodes becomes an essential step in CRNs because of the nature of the CR technology, which permits unlicensed users to access the frequency bands of the licensed users, taking into consideration that they do not interfere with the licensed users. The spectrum access strategies have some features such as their dynamicity and flexibility, which make it a pressing need for designing communication approaches and schemes

The associate editor coordinating the review of this manuscript and approving it for publication was Amjad Mehmood.

that discover and use the spectrum holes. With this method, the interference between the communicating nodes will be minimized, the contention on channels will decrease, and the average channel efficiency will improve. Routing in CRNs is different from the traditional routing protocols due to several challenges. These challenges are related to two factors: the CR technology itself and the environment where the CR is applied. The former influences the dynamic changes of the spectrum availability and the instable behavior of spectrum users, while the latter influences the resources' heterogeneity and the ability of synchronizing the different spectrum users. Thus, applying the traditional routing protocols used in the ad-hoc networks in the CRNs will result in a poor network performance in terms of higher end-to-end delay, less packet delivery ratio, more packet loss ratio, and low throughput.

Many security attacks (both passive and active) can target the CRNs, especially during the spectrum sensing phase in multiple ways. Firstly, the radio technology itself can be attacked since any radio frequency can be blocked or jammed when nodes transmit adequate signals at the same frequency with enough power. Secondly, the absence of the control over the unlicensed users' behavior threatens the security of the licensed users. Therefore, while designing routing algorithms or protocols for CRNs, security must be enhanced in two ways. The first is by making sure that the routing algorithm or protocol itself is secure, that is, securing the route establishment, route maintenance, and data forwarding processes by applying cryptographic encryption to the different messages transmitted over the available routes. The second way is by using security as a routing metric to find the best path(s) that contain(s) the best secure nodes which, to the best of our knowledge, has not been applied in the CRNs to date.

In this paper, which is an extension of our previous work in [5], [6], nodes' behavior during the spectrum sensing phase is analyzed to propose a compound secure routing algorithm used in the spectrum management phase. It uses the nodes' belief level (BL), which measures the level of security of the nodes' behavior during the spectrum sensing phase. The proposed routing algorithm combines security (nodes' BL) as a routing metric with two other routing metrics, which are the probability of PU presence and channel cost in terms of delay. In the proposed algorithm, we rely on two key-cryptographic methods: the public-key and symmetric-key cryptography. These two cryptographic methods are used to encrypt/decrypt the messages transmitted during the route establishment, route maintenance, and data forwarding phases. Therefore, these cryptographic methods prevent any malicious node from eavesdropping on these messages, from altering them, and/or from participating in the packets routing over the network. The objective of the proposed approach is to build secure routes that contain trusted nodes only, which would enhance the network performance in terms of end-to-end delay, packet delivery ratio, packet loss ratio, and routing overhead.

The main contributions of this paper and the characteristics of the proposed approach can be summarized as follows:

- To the best of our knowledge, this work is the first to consider security as a routing metric in the CRNs. In the proposed approach, security covers two disciplines: providing resources' access to secure nodes only and securing the message exchange process over the network. By doing so, we secure the network paths, thereby enhancing the network security and performance implicitly.
- To the best of our knowledge, this work is the first to combine the spectrum sensing and the spectrum management phases in the CRNs. It uses the nodes' behavior during the spectrum sensing phase to find the best secure routes during the spectrum management phase.
- The proposed approach works as a proactive scheme to detect misbehaving nodes before the start of data transmission process.
- In the proposed approach, the best paths are found based on three different routing metrics combined: the nodes' BL, the probability of PU presence, and the channel cost.
- The three metrics used in the proposed routing approach have different weights for finding the best paths based on their effects on the routing process. The proposed approach focuses more on the nodes' BL, which is the main metric of the proposed routing algorithm.
- The proposed approach has the ability of adapting any changes in the licensed users' activity over the network, which is being implemented by considering the probability of the PU's presence to be a routing metric. Hence, the available routes will be more stable, which would make the proposed approach more reliable.
- The proposed approach considers the issues happening at the different layers of the OSI architecture, that is, it is a cross-layering approach. It considers the channel status and the PU's activity at the physical and data link layers, which affects the routes establishment at the network layer. Therefore, it implicitly minimizes the time needed for route(s) establishment and reduces the maintenance cost.
- The proposed algorithm is evaluated from different perspectives: its security functionality, its correctness, and its performance. This proves that it is secure against attacks and outperforms other approaches.

The rest of this paper is further organized into six additional sections. Section II presents a literature review. In Section III, the proposed scheme is shown in detail. A case study is presented in Section IV. In Section V, the performance of the approach and evaluation results are presented, which show the efficiency of the proposed routing algorithm as compared with other algorithms/protocols. The proposed algorithm is validated and verified in Section VI. The paper is concluded in Section VII.

## II. RELATED WORK

Two different routing infrastructures are used in conventional networks: single-hop infrastructure and multi-hop infrastructure [6]. In the single-hop infrastructure, there is only one

single path that exists between any two communicating nodes in the network. This single path is used for packets transmission between the communicating nodes. Its main advantage is that the routing tables are simpler and the packets flow smoothly. However, the single-hop infrastructure is not fault-tolerant. In other words, if any failure occurs in the network, the nodes become unreachable, and messages transmitted to them are dropped and not sent successfully. This is its main drawback. On the other hand, the multi-hop infrastructure is fault-tolerant because of the availability of multiple paths between any two communicating nodes. If any failure occurs in the network, the packets still have the chance of being sent successfully to their destination because of back-up paths that can be used for message delivery. The main drawback of multi-hop infrastructure is its complicated implementation that makes the routing tables much bigger. Both the infrastructures can be applied in CRNs. They can use the classical routing metrics such as delay, hop count, distance, or power consumption [7]. New routing metrics that have been introduced based on the CRN characteristics such as spectrum availability, SU interference, or route stability can also be used to find the best routes [8].

The end-to-end delay is a routing metric used in the classical networks. Many factors affect the end-to-end delay, such as queuing delay, transmission delay, and channel switching time. The authors of [9] proposed a spectrum-aware routing scheme for infrastructure-based CRN called SAAR. This scheme uses statistical information about the network to find the quality of any path routing for each network node. The time required to change the channel and the back-off delay caused by the contention between the different nodes are used to develop another routing metric in [10]. In [11], the authors find the optimal path between any nodes based on various metrics such as delay, channel availability, and the probability of PUs' interference. The main drawback of such protocols is that they may not be practical if cognitive nodes do not follow protocol's presumptions. The time required to change the channel is proportional to the difference between the initial and final channels. The queuing delay has been taking into consideration with the previous concepts of delay by proposing another routing algorithm in [12], [13]. In [14], a routing algorithm called SEARCH, which uses the delay as a routing metric, is proposed. It applies the end-to-end delay as a routing metric, which includes the cost of switching channels and the delay over each channel. In [15], the authors proposed another routing protocol called spectrum aware opportunistic routing (SAOR). It relies on a routing metric called the opportunistic link transmission (OLT) that uses three delay concepts: link transmission delay, packet queuing delay, and link access delay. The authors in [16] proposed a routing protocol that relies on location information and channel usage statistics. It uses a routing metric called cognitive transport throughput (CTT), which represents the potential relay gain over the next hop. Another routing protocol called DORP [12] proposes a delay aware routing metric. It considers different types of delays, such as queuing delay, switching delay, and back-off or medium access delay, in finding the best path(s). The path with the minimum combined delay value is selected for routing.

Another routing metric that is widely applied in different routing algorithms is the hop count. The hop count is used as a routing metric in Ad Hoc On-Demand Distance Vector protocol (AODV) [17], Cognitive Ad Hoc On-Demand Distance Vector protocol (CAODV) [18], and Spectrum Aware Mesh Routing (SAMER) [19] routing protocols. In AODV or in CAODV, which is an adapted version of AODV for CRNs, the regions that have active PUs are eliminated during the route establishment and data forwarding phases; therefore, the best path is the one that has no active PUs. SAMER protocol utilizes available spectrum blocks by routing data traffic over paths with higher spectrum availability; therefore, the best path is the one that has the highest spectrum availability. The authors in [20] proposed an on-demand routing scheme called split multi-path routing (SMR). It establishes different paths between any two network nodes, wherein one of these paths has the shortest delay path. An on-demand node-disjoint routing algorithm (NDMR) is proposed in [21]. It builds different node-disjoint routes with a low routing overhead. Differential queue backlog is used as a routing metric in [22]. It is applied to achieve throughput efficiency by proposing a distributed medium access control algorithm. In CRNs, the transmission delay time is affected by many factors such as the data transmission time, spectrum sensing time, and presence of PU over its channels. In contrary, such factors may also affect the network security, as a malicious node can emulate a PU in order to lower the network performance [23], [24].

Power consumption is considered to be a routing metric in many routing algorithms. If the power consumption-based routing algorithm is applied in CRNs, then the best path is the one that uses less power for packets transmission. Another routing protocol, namely MP-JSRA, is proposed in [25]. It uses the lowest Data Transmission Cost (DTC) as a routing metric. The mobility cost and the interference cost to the other network nodes, including PUs and Sus, are the two factors used to find the lowest DTC, which is then used to find the best route. The authors in [26] proposed an energy harvesting routing model for multi-hop CRN. This model used Q learning with Reinforcement Learning (EHR-QL) to find optimal paths. Another routing protocol, namely LAUNCH, is proposed in [27]. It uses multiple routing metrics: PU activity, switching delay, and location information, as routing metrics. The authors in [28]–[30] studied routing algorithms for energy harvesting in multi-hop wireless networks. The main drawback of such protocols is that they consume a large amount of router resources, as each node must keep track of the network global state. The proposed scheme in [30] focuses on minimizing the probability of an outage in an energy harvesting multi-hop CRN by considering the joint power allocation and routing selection. The best route path is selected based on The Bellman-Ford algorithm and Dijkstra's algorithm.

Many cryptographic security frameworks for data mobility or nodes transmission have been proposed in several environments such as MANETs, VANETs, UAVs, WMNs, and WSNs [31]–[34]. Such frameworks cannot be directly applied in CRNs because of their unique individuality. Additionally, these current cryptographic techniques increase the transmission delay, which may lead to an increase in the communication and storage overhead. In CRNs, nodes identity verification can be done using trust-based approaches [35]–[39]. General cryptographic algorithms such symmetric key and public key can be used in CRNs. Trust-based approaches improve the network security without affecting the network delay and communication overhead. However, such trust-based security methods in CRNs are still developing. Therefore, a new trust-based method is proposed in this paper, which uses trust values to develop a secure routing protocol.

The main limitation of the previous work is that none of them has considered security a routing metric. Security has been investigated in detecting nodes that degrade the network performance. Existing solutions are reactive approaches, wherein nodes are detected after they start their malicious behavior during the data transmission phase. The major scientific novel contribution of this paper is using security as a routing metric to find the best secure paths for data transmission between the different network nodes. Security in the proposed routing algorithm relies on nodes' behavior during the spectrum sensing process. Therefore, the proposed approach works as a proactive solution, as it can identify the misbehaving nodes during the spectrum sensing phase and before the data transmission phase starts. The main goal of the paper is to provide efficient and secure spectrum sensing scheme for better data transmission and secure spectrum management. All routing algorithms differ from each other in the routing metric used, the environment where the protocol is applied, and the performance.

The main difference between our proposed routing algorithm and the previously mentioned routing algorithms or protocols is that ours is the first work that uses security as a routing metric in CRNs, combines the spectrum sensing and the spectrum management phases, and has better performance measures as compared with other routing protocols in terms of end-to-end-delay, packet delivery ratio, packet loss ratio, and routing overhead. Moreover, to the best of our knowledge, the proposed routing algorithm is the first to be validated in terms of security functionality in CRNs.

## III. THE PROPOSED APPROACH

In this section, we have shown the network model, the general assumptions applied to our proposed approach, as well as the proposed routing algorithm in detail.

### A. PREFACE

Figure 1 shows the system model, which is a network of $M$ secondary users (SUs) grouped into $L$ different clusters based on their geographical locations as in [40]. One central point called fusion center (FC) controls the traffic over the network and manages the communication in the network clusters. In each cluster, the FC selects the node that has the highest BL as a cluster head (CH). More details on the clustering method, CH selection method, and its constraints can be found in [41]. We assume that the CH cannot become malicious once selected.

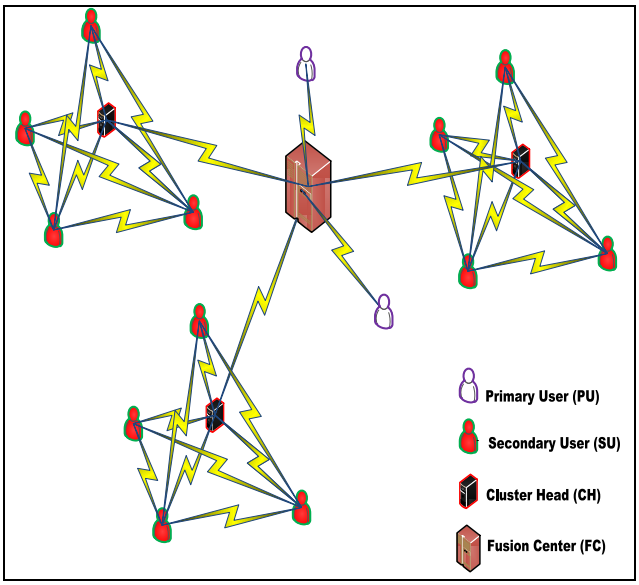


**FIGURE 1.** System Model.

The nodes' BL measures the degree of security of the nodes' behavior during the spectrum sensing phase. The attacker model and capability are like the one that we proposed and used in [42], wherein the node may behave in a malicious, misbehaving, cheating, and/or selfish way to launch different attacks such as PUEA, SSDF, DoS, and objective function attack.

An initial moderate BL of value equal to two is assigned to each node at the joining time. We assume four categories of trust, and the BL has a range of [0–4] based on these categories of trust as following:

$$0 \leq BL \leq 1 : Very\_Untrusted$$
$$1 < BL < 2 : Untrusted$$
$$2 \leq BL < 3 : Trusted$$
$$3 \leq BL \leq 4 : Very\_Trusted$$

As each node is assigned an initial moderate BL of value equal to two, it is in the "Trusted" category. The cooperative spectrum sensing is done as in [43], wherein all the cluster nodes sense the spectrum, make a decision about the PU presence/absence and forward their decision to the other nodes. Upon reception of the sensing decision from other neighboring nodes, each SU prepares a report called sensing-reputation report (described in Section III b) and sends it to the CH.

We have developed a hybrid routing algorithm that uses security (nodes' BL) combined with other routing metrics to

find the best path(s) between any two communicating nodes in a cluster. The proposed routing algorithm considers three metrics: channel cost in terms of delay, probability of PU presence, and node's belief level. The proposed approach has an objective function—to maximize the node's belief level, simultaneously minimizing the PU's presence probability and channel cost. The messages sent between the different network nodes during the spectrum sensing phase and spectrum management phase are encrypted by using the symmetric-key cryptography. Symmetric key has many advantages; it is straightforward, occupies less memory, uses less memory, and utilizes less power. Preventing misbehaving sensing nodes from participating in the spectrum sensing phase and accessing the network helps to fairly allocate and manage the network resources. Consequently, the spectrum security and utilization are increased. Public-key cryptography is initially used to encrypt the messages sent between the joining node and the authenticating node. Once a symmetric key is shared between the joining node, the FC, and the CH, all the messages from then on are encrypted by this symmetric key. The symmetric key can be assigned to each node during the node's authentication process which can be achieved as in [41]. During the spectrum sensing and the spectrum management phases, each node uses the same key for encrypting and decrypting the messages transmitted.

### B. MONITORING NODES' BEHAVIOR IN SPECTRUM SENSING

In each cluster, each node senses the spectrum to find any unused spectrum channels. The sensing method used is the energy detection technique [43], wherein each sensing node uses its sensing information to make the initial binary decision about the presence/absence of PU in its reserved channel(s). Each sensing SU compares the pre-known information about the PUs' signal (such as signal power threshold and modulation type) with the sensing signal recorded over a specific PU's channel in order to avoid malicious nodes that emulate PUs. If the signals do not match, the sensing SU decides that a malicious node is emulating PU; therefore, the sensing SU sends a broadcast message to notify all the cluster nodes. However, if they match, the sensing SU decides that a real PU is present in its spectrum channels. If no signal is received over the sensing channel(s), the sensing SU decides that no PU is present, and that the spectrum can be used.

The spectrum sensing process is a periodic process, that is, it is carried over multiple sensing rounds. We assume that each sensing round is carried over 200$ms$. Therefore, every sensing node must finish sensing within the sensing round as at every sensing round, each sensing SU saves its sensing decision in a parameter called sensing result (SR) and forwards it to its neighbors. Meanwhile, each sensing SU receives the SR(s) of its neighbors. Then, each sensing SU monitors the behavior of its neighboring nodes during the spectrum sensing phase by comparing its own SR with the received SR from its neighboring node(s). If they match, the sensing SU decides that the behavior of its neighboring node(s) is "GOOD"; otherwise, it is "BAD." Finally, each sensing SU prepares a report called the sensing-reputation report and forwards it to the CH. The sensing-reputation report has the following format and information: *Reporting Node ID (RG)* || $SR_{RG}$ || *Reported Node ID (RD)* || *Opinion*, where $SR_{RG}$ is the sensing result of the reporting node, which is either 0 (i.e. "*Free*" spectrum) or 1 (i.e. "*Occupied*" spectrum), and Opinion is about the reported node (RD), which is either 0 (i.e. "BAD" node) or 1 (i.e. "GOOD" node).

The CH collects the sensing-reputation reports sent by the different sensing SUs and analyzes them to make two decisions. The first decision is about the spectrum availability, and the second decision is about the behavior of each sensing SU. Then, the CH forwards the final decision about the spectrum availability to its cluster nodes, while the CH applies proper reward/penalty actions to the sensing SUs based on their behavior decision. A specific rule is applied by the CH to process these reports in order to make the decision about the behavior of the reporting and reported nodes. The general rule is *K-out-of-N* rule, wherein K users out of N users must have the same opinion in order to consider their opinion. In case the 50% K-rule is used, K is equal to N/2. We have proposed a new K-rule, where K represents the number of votes. Each cluster node is assigned a different voting weight based on its BL value. The following criteria are applied in order to find the value of K based on the four categories of BL mentioned before:

- A node's decision is worth three votes if its BL value is in the range of $3 \leq BL \leq 4$.
- A node's decision is worth two votes if its BL value is in the range of $2.5 \leq BL < 3$.
- A node's decision is worth one vote if its BL value is in the range of $2 \leq BL \leq 2.5$.
- A node's decision is worth zero votes if its BL value is less than 2.

Then, the CH updates the belief level of each node based on the number of the "*GOOD*" or "*BAD*" opinions received from the different sensing SUs. Each "*GOOD*" behaving node will be rewarded with an increase in its BL, and each "*BAD*" behaving node will be penalized with a decrease in its BL. The CH uses a parameter called Adjustment Factor (AF), which is calculated as shown in (1), and then adds it to the recent value of BL as shown in (2). The AF of a node represents the difference between the "GOOD" opinions and the "BAD" opinions sent by the reporting nodes about the reported node.

$$\begin{aligned} att &= t_{update} \\ AF_{SU_i} &= \left( \sum_{g=1,\neq i}^{G} \propto * \mathbb{N}(BL_{SU_g}) \right) \\ &\quad - \left( \sum_{b=1,\neq i}^{B} \beta * \mathbb{N}(BL_{SU_b}) \right) \end{aligned} \tag{1}$$

$$\left(BL_{SU_i}\right)_{t_{update}} = \left(AF_{SU_i}\right) + \left(BL_{SU_i}\right)_{t_{update-1}} \quad s.t. -4 \leq AF \leq 4 \tag{2}$$

where $G$ represents the number of nodes which decide that $SU_i$ is a good node, $B$ represents the number of nodes which decide that $SU_i$ is a bad node, $\propto$ is the rewarding factor and $\beta$ is the penalizing factor, $\mathbb{N}(BL_{SU_b})$ is the normalized belief level of the reporting node that sends a "BAD" opinion about $SU_i$, and $\mathbb{N}(BL_{SU_g})$ is the normalized belief level of the reporting node that sends a "GOOD" opinion about $SU_i$. We choose the rewarding factor and the penalizing factor, and as in real life, the penalty has more weight than rewarding.

The AF value limits cannot be more than 4 or less than $-4$ because the BL range is between zero and four; therefore, the updated value of BL after adding the AF value should remain within the valid range. If AF value is more than 4, it will be set to 4, and if it is less than $-4$, it will be set to $-4$. Each sensing node's BL affects the process of finding the value of AF; the higher the reporting node's BL, the greater the effect on the AF value. Once the final BL of each node is calculated, it is used as a routing metric combined with other routing metrics. If a node with a BL of 4 becomes malicious, the periodic sensing process, that is, the periodic voting of all nodes allows all affected nodes to detect this node as malicious, thereby decreasing its BL value; and all the nodes come to identify it as malicious, and it gets reported to the CH.

### C. THE ROUTING ALGORITHM

The main objective of the proposed routing algorithm is to find the best path between any two communicating nodes. As mentioned earlier, the best next nodes have the highest BL, the lowest probability of PU presence, and the lowest channel cost will be forming the best path. The objective function of finding the best next node (BNN) for each node is found as in (3):

$$F\left(BNN\right) = \max\left(BL_{Node}\right) + \min\left(Cost_{ch}\right) + \min\left(P_{PU}\right) \tag{3}$$

where $F(BNN)$ is the function of the best next node, $BL_{SU_j}$ is the next node's BL, $P_{PU}$ is the probability of PU's presence over next channel, and $Cost_{ch}$ is the cost of the channel between current node and its next node, which is the delay in our proposed routing algorithm.

Algorithm $I$ is showing the proposed routing approach step by step. All the parameters and the functions used to implement the algorithm are initially defined. The algorithm starts when every CH sends the following information to its cluster nodes: the BL of their next node(s), the channel(s) cost, and the probability of PU presence over those channels. Then, each current cluster node ($SU_i$) uses the BL of its next nodes(s) to find the inverse BL as $BL_{SU_j}^{inverse} = 1/BL_{SU_j}$. Those inverse BLs along with the channel(s) cost and the probability of PU presence over those channels are saved in a table called Next Nodes Information (NNI) as shown in Table 1. Each node ($SU_i$) has its own NNI table that the node uses

**Algorithm 1** The Routing Algorithm

**Parameters:**

$M$ : the set of SUs.
$X$ : a subset of M that represents the next nodes of the current node.
$K$ : a set of Channels.
$Cost_{ch}$ : the Channel's cost.
$SU_{src}$ : the source node.
$SU_{des}$ : the destination node.
$SU_{cur}$ : the current node.
$SU_{next}$ : the next node.
$SU_{best}$ : the best next node.
$K_{cur\rightarrow next}$ : the channel between the current node and its next node.
$\text{Cost}_{\text{K}_{\text{cur}\rightarrow next}}$ : the cost of the channel between the current node and its next node.
$BL_{Node}^{inverse}$ : the node's inverse BL.
$P_{PU}$ : the probability of PU's presence.
$V_{SU}$ : the calculated value in the objective function.
Next Nodes Information (NNI) Table: a table maintained by the current SU, which includes information about its neighboring (next) nodes: Node ID, Inverse BL, Channel Cost, and Probability of PU Presence.
Save (Inverse BL, Channel Cost, and Probability of PU Presence): a function applied by the current SU to save the information of its next nodes in NNI.
$BPath(BNN)$ : a function that builds the best path between any two nodes by appending the best next node of each node in the path.

**Initialize**

For each $SU_i \in M$
  $SU_{cur} = SU_i$
  For each $SU_j \in X$
    $SU_{next} = SU_j$
    $BL_{next}^{inverse} = 1/BL_{SU_{next}}$
    $Save(BL_{SU_{next}}^{inverse}, Cost_{K_{cur\rightarrow next}}, P_{PU})$
  Endfor
Endfor

**Sort of Next Nodes**

For each $SU_{cur} \in M$
  For each $SU_{next} \in X$
    $Sort\left(BL_{SU_{next}}^{inverse}\right)$
    $Sort\left(Cost_{K_{cur\rightarrow next}}\right)$
    $Sort(P_{PU})$
  Endfor
Endfor

**Finding the Best Next Node**

For each $SU_i \in M$
  For each $SU_{next} \in X$
    $findV_{SU_{next}} = \left(\mu * Order\left(BL_{SU_{next}}^{inverse}\right)\right) + \left(\varepsilon * Order\left(Cost_{K_{cur\rightarrow next}}\right)\right) + \left(\vartheta * Order(P_{PU})\right)$
  Endfor
  $small = MIN(V_{SU})$
  $BNN = IndexOf(small)$

**Algorithm 1** *(Continued.)* The Routing Algorithm

**Build the Best Path**

*BPathBNN*

Endfor

**Special Cases:**

1. If the current node has multiple nodes as BNN, i.e. multiple nodes have the same $V_{SU_{next}}$:
   - The current node chooses the neighboring node that has $MIN(BL^{inverse}_{SU_{next}})$.
   - If multiple nodes have the same $BL^{inverse}_{SU_{next}}$, the current node chooses the neighboring node that has $MIN(P_{PU})$.
   - If multiple nodes have the same $P_{PU}$, the current node chooses the neighboring node that has $MIN(Cost_{K_{cur\rightarrow next}})$.
   - If multiple nodes have the same $BL^{inverse}_{SU_{next}}$, $P_{PU}$, and $Cost_{ch_{cur\rightarrow next}}$, the current node chooses any of the neighboring nodes.
2. If $P_{PU}$ over a channel is equal to 1, this channel is eliminated from the routes' establishment.

**TABLE 1.** Next nodes information (NNI).

| Next Node ID | Inversed BL | Channel Cost | Probability of PU Presence |
|---|---|---|---|

to find its best next node among its different neighboring nodes. Then, every ($SU_i$) arranges its neighboring nodes according to each parameter in an ascending order by using the *Sort* (*Parameter*) function. After that, every ($SU_i$) applies the weight coefficient of each parameter to the nodes' order in order to find a value called $V_{SU_j}$, which will be used to find the best next node. The objective function, as shown in (4), is used to find the best next node. According to the objective function, the best next node is the node that has the smallest $V_{SU_j}$. Finally, all the best next nodes are appended together to form the best path.

$$F(BNN) = MIN(\left(\mu * Order\left(BL^{inverse}_{SU_j}\right)\right) + (\varepsilon * Order(Cost_{ch})) + (\vartheta * Order(P_{PU})) \quad (4)$$

Each metric has a weight coefficient that represents how much important the metric is in finding the best path. We have defined the following weight coefficients:

- $\mu$ is the weight coefficient of the BL parameter and equals to 0.5.
- $\varepsilon$ is the weight coefficient of the channel cost parameter and equals to 0.2.
- $\vartheta$ is the weight coefficient of the probability of PU presence parameter and equals to 0.3.

The values of weight coefficients were selected to satisfy the main objective of the routing algorithm—to use security as a routing metric. Therefore, the BL value has the highest priority (i.e. its weight coefficient has the highest value) followed by probability of PU presence, and finally the channel cost. The sum of these weight coefficients equals to one (i.e. $\mu + \varepsilon + \vartheta = 1$).

### D. COMPLEXITY ANALYSIS

In this section, the complexity of the proposed routing algorithm is discussed including the sensing phase. The complexity is evaluated in terms of the communication overhead (i.e. the number of messages exchanged) and storage overhead (i.e. memory usage). First, for the communication overhead, the messages are exchanged between all sensing nodes and the CH. Sensing-reputation reports are sent by each cluster sensing node to its CH. The neighboring nodes' information are forwarded by the CH to each cluster node, which in turn saves this information in the NNI table. Supposedly, if we have a cluster of $N$ SUs, and each SU has certain neighboring nodes denoted by '$M$,' then number of messages exchanged by sensing nodes to their CH can be given approximately as $N * M$, where $N$ is the number of messages CH sends which is equal to number of SUs. Therefore, the total messages exchanged can be given approximately as $N * M + N$, which is a complexity of second order ($\approx O(N^2)$).

Second, with respect to the memory usage, $\boldsymbol{N * N}$ entries of memory are required by each CH to store all the cluster nodes' information, where $\boldsymbol{N}$ is number of SUs in the cluster. On the other hand, $\boldsymbol{M}$ entries of memory are required by each cluster node to save its neighboring nodes' information, where $\boldsymbol{M}$ is the number of the neighboring nodes of an SU. Hence, the total memory usage can be represented approximately as $\boldsymbol{N * N + N * M}$, which is a complexity of second order ($\approx \boldsymbol{O(N^2)}$). The memory utilization in addition to the processing time at the CH level would increase if the number of SUs in the network raises.

## IV. CASE STUDY

In this section, we have presented a case scenario in order to show how our proposed routing algorithm works. Figure 2 shows the network scenario. In Table 2, each node's information is shown: its ID, its BL, its neighbors, the channel cost, and the probability of PU presence over each channel, with the assumption that there is at least one channel between each two SUs. We assume that $SU_0$ is the source node and $SU_{18}$ is the destination node, therefore the best path(s) will be found by applying our proposed algorithm. According to the proposed algorithm, each node will first find its best next hop, and then each next hop is added to a list that contains all best next nodes. When these nodes accumulate in the list in this manner, the best path is formed.

**At the source node ($SU_0$):**

The source node, $SU_0$, has two neighboring nodes: $SU_1$ and $SU_2$. It must choose either one as its next node. The source node, $SU_0$, performs the following calculations based on the routing algorithm:

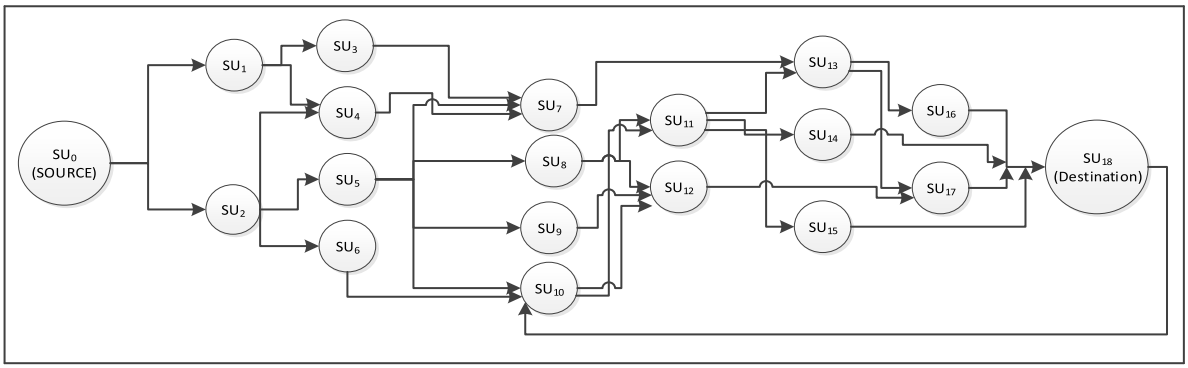


**FIGURE 2.** A Routing Scenario.

**TABLE 2.** The routing metrics values used for the scenario.

| Node ID | Node's BL | Neighbor node(s) | Channel Cost(delay) | PU's presence probability over that channel |
|---|---|---|---|---|
| 0 | 3.4 | 1,2 | 9, 6 | 0.4, 0.52 |
| 1 | 2.8 | 3,4 | 6, 3 | 0.36, 0.29 |
| 2 | 3.8 | 4,5,6 | 8, 7, 4 | 0.18, 0.43, 0.72 |
| 3 | 2.4 | 7 | 5 | 0.25 |
| 4 | 3 | 7 | 3 | 0.74 |
| 5 | 3.7 | 7, 8, 9, 10 | 3, 5, 6, 4 | 0.16, 0.24, 0.31, 0.36 |
| 6 | 2.5 | 10 | 12 | 0.17 |
| 7 | 2.4 | 13 | 9 | 0.81 |
| 8 | 3.4 | 11,12 | 4, 3 | 0.31, 0.19 |
| 9 | 2.7 | 12 | 3 | 0.23 |
| 10 | 2.8 | 11,12 | 6,9 | 0.54, 0.19 |
| 11 | 3.7 | 13, 14, 15 | 4, 8, 2 | 0.34, 0.21, 0.76 |
| 12 | 3.3 | 17 | 3 | 0.41 |
| 13 | 3 | 16, 17 | 5, 2 | 0.34, 0.12 |
| 14 | 2.5 | 18 | 8 | 0.43 |
| 15 | 2.7 | 18 | 16 | 0.27 |
| 16 | 2.6 | 18 | 4 | 0.68 |
| 17 | 2.5 | 18 | 5 | 0.19 |
| 18 | 3.4 | 10 | 3 | 0.35 |

| Next Node ID | ~~BL Inverse~~ →order | ~~Channel cost~~ →order | ~~Prob. of PU presence~~ →order | $V_{SU}$ |
|---|---|---|---|---|
| $SU_1$ | ~~0.36~~ →2 | ~~9~~ →2 | ~~0.40~~ →1 | ~~0~~ →1.7 |
| $SU_2$ | ~~0.26~~ →1 | ~~6~~ →1 | ~~0.52~~ →2 | ~~0~~ →1.1 |

According to the objective function and the routing algorithm, the best next node is the node that has the smallest $V_{SU_j}$, therefore; the source node, $SU_0$, chooses $SU_2$ as its best next hop.

**The best path includes $SU_0 \rightarrow SU_2$**

**At $SU_2$**

$SU_2$ has three neighboring nodes: $SU_4$, $SU_5$, and $SU_6$. It must choose one of them as its next node. Hence, $SU_2$ does the following calculations based on the routing algorithm:

| Next Node ID | ~~BL Inverse~~ →order | ~~Channel cost~~ →order | ~~Prob. of PU presence~~ →order | $V_{SU}$ |
|---|---|---|---|---|
| $SU_4$ | ~~0.33~~ →2 | ~~8~~ →3 | ~~0.18~~ →1 | ~~0~~ →1.9 |
| $SU_5$ | ~~0.40~~ →1 | ~~7~~ →2 | ~~0.43~~ →2 | ~~0~~ →1.5 |
| $SU_6$ | ~~0.27~~ →3 | ~~4~~ →1 | ~~0.72~~ →3 | ~~0~~ →2.6 |

According to the objective function and the routing algorithm, the best next node is the node that has the smallest $V_{SU_j}$, therefore; $SU_2$ chooses $SU_5$ as its next hop.

**The best path includes $SU_0 \rightarrow SU_2 \rightarrow SU_5$**

**At $SU_5$**

$SU_5$ has four neighboring nodes: $SU_7$, $SU_8$, $SU_9$, and $SU_{10}$. It must choose one of them as its next node. Hence, $SU_5$ does the following calculations based on the routing algorithm:

| Next Node ID | ~~BL Inverse~~ →order | ~~Channel cost~~ →order | ~~Prob. of PU presence~~ →order | $V_{SU}$ |
|---|---|---|---|---|
| $SU_7$ | ~~0.42~~ →4 | ~~3~~ →1 | ~~0.16~~ →1 | ~~0~~ →2.5 |
| $SU_8$ | ~~0.29~~ →1 | ~~5~~ →2 | ~~0.24~~ →2 | ~~0~~ →1.5 |
| $SU_9$ | ~~0.37~~ →3 | ~~6~~ →4 | ~~0.31~~ →3 | ~~0~~ →3.2 |
| $SU_{10}$ | ~~0.36~~ →2 | ~~4~~ →3 | ~~0.36~~ →4 | ~~0~~ →2.8 |

According to the objective function and the routing algorithm, the best next node is the node that has the smallest $V_{SU_j}$, therefore; $SU_5$ chooses $SU_8$ as its next hop.

**The best path includes $SU_0 \rightarrow SU_2 \rightarrow SU_5 \rightarrow SU_8$**

**At $SU_8$**

$SU_8$ has two neighboring nodes: $SU_{11}$ and $SU_{12}$ as its next node. It must choose either one as its next node. Hence,

$SU_8$ does the following calculations based on the routing algorithm:

| Next Node ID | ~~BL Inverse~~ →order | ~~Channel cost~~ →order | ~~Prob. of PU presence~~ →order | $V_{SU}$ |
|---|---|---|---|---|
| $SU_{11}$ | ~~0.27~~ →1 | ~~4~~ →2 | ~~0.31~~ →2 | ~~0~~ →1.5 |
| $SU_{12}$ | ~~0.30~~ →2 | ~~3~~ →1 | ~~0.19~~ →1 | ~~0~~ →1.6 |

According to the objective function and the routing algorithm, the best next node is the node that has the smallest $V_{SU_j}$, therefore; $SU_8$ chooses $SU_{11}$ as its next hop.

**The best path includes $SU_0 \rightarrow SU_2 \rightarrow SU_5 \rightarrow SU_8 \rightarrow SU_{11}$**

**At $SU_{11}$**

$SU_{11}$ has three neighboring nodes: $SU_{13}$, $SU_{14}$, and $SU_{15}$. It must choose one of them as its next node. $SU_{11}$ does the following calculations based on the routing algorithm:

| Next Node ID | ~~BL Inverse~~ →order | ~~Channel cost~~ →order | ~~Prob. of PU presence~~ →order | $V_{SU}$ |
|---|---|---|---|---|
| $SU_{13}$ | ~~0.33~~ →1 | ~~4~~ →2 | ~~0.34~~ →2 | ~~0~~ →1.5 |
| $SU_{14}$ | ~~0.40~~ →3 | ~~8~~ →3 | ~~0.21~~ →1 | ~~0~~ →2.4 |
| $SU_{15}$ | ~~0.37~~ →2 | ~~2~~ →1 | ~~0.76~~ →3 | ~~0~~ →2.1 |

According to the objective function and the routing algorithm, the best next node is the node that has the smallest $V_{SU_j}$, therefore; $SU_{11}$ chooses $SU_{13}$ as its next hop.

**The best path includes $SU_0 \rightarrow SU_2 \rightarrow SU_5 \rightarrow SU_8 \rightarrow SU_{11} \rightarrow SU_{13}$**

**At $SU_{13}$**

$SU_{13}$ has two neighboring nodes: $SU_{16}$ and $SU_{17}$ It must choose either one as its next node. Hence, $SU_{13}$ does the following calculations based on the routing algorithm:

| Next Node ID | ~~BL Inverse~~ →order | ~~Channel cost~~ →order | ~~Prob. of PU presence~~ →order | $V_{SU}$ |
|---|---|---|---|---|
| $SU_{16}$ | ~~0.38~~ →1 | ~~5~~ →2 | ~~0.34~~ →2 | ~~0~~ →1.5 |
| $SU_{17}$ | ~~0.40~~ →2 | ~~2~~ →1 | ~~0.12~~ →1 | ~~0~~ →1.5 |

According to the objective function and the routing algorithm, the best next node is the node that has the smallest $V_{SU_j}$, therefore; $SU_{16}$ and $SU_{17}$ are both the best next node for $SU_{13}$. However, $SU_{13}$ must choose one of them. In this case, the cluster node that has a higher BL is chosen as the next node, therefore; $SU_{16}$ is selected as the next node of $SU_{13}$.

**The best path includes $SU_0 \rightarrow SU_2 \rightarrow SU_5 \rightarrow SU_8 \rightarrow SU_{11} \rightarrow SU_{13} \rightarrow SU_{16}$**

**At $SU_{16}$**

$SU_{16}$ has one neighboring node only which is $SU_{18}$. Therefore, it is the next node for $SU_{16}$.

**The best path is $SU_0 \rightarrow SU_2 \rightarrow SU_5 \rightarrow SU_8 \rightarrow SU_{11} \rightarrow SU_{13} \rightarrow SU_{16} \rightarrow SU_{18}$**

Hence, the route shown above is the best and secured route, which guarantees that no adversary node can overhear or alter. If a message is sent over this route, the nodes in the route should forward the message to its next hop with no problems assuming that the channels are free of error prone.

## V. PERFORMANCE EVALUATION

### A. PERFORMANCE METRICS UNITS

We have evaluated the performance of our proposed approach by considering multiple performance metrics. The proposed routing algorithm is simulated in three different networks, each of which has a different number of SUs. Then, we compare the performance of our proposed approach with three other routing algorithms in terms of different metrics:

- *Average end-to-end delay* (measured in seconds) represents the total time needed for a packet to be received by the destination node after it has been generated at the source node.
- *Packet delivery ratio* measures the ratio of the number of packets received by the destination node to the number of packets generated by the source node.
- *Packet loss ratio* measures the packets that have been generated and transmitted by the source node, but not received by the destination node.
- *Routing overhead* measures the ratio of routing packets to the total number of packets sent over the network.

It is worth mentioning that we considered both packet delivery ratio and packet loss ratio as a packet considered lost if it was delivered after its deadline; therefore, packet loss ratio gives us indications if attacks are delaying the delivery of packets, which, in turn, helps in identifying such nodes, thereby helping in mitigating attacks.

### B. SIMULATION ENVIRONMENT SETUP

We simulated our routing algorithm in the QualNet environment and analyzed the results through MATLAB. We simulated our proposed approach under two different simulation scenarios. Tables 3 and 4 show the simulation parameters used referring to [41]–[45]. In the first simulation scenario shown in Table 3, we compared our proposed routing algorithm with three different state-of-the-art routing algorithms used in CRNs: COADV [18], SEARCH [14], and LAUNCH [27]. In the second simulation scenario shown in Table 4, we compared the proposed approach with two other routing protocols: DORP [12] and AODV [17]. Note that we did not simulate the other routing algorithms; we just used their results as shown in their research papers. The rationale behind using these previous mentioned routing algorithms in the comparison with the proposed approach is to compare their general performance regardless of the routing metrics used in each.

### C. NUMERICAL RESULTS AND PERFORMANCE COMPARISON

This section shows the performance comparison between the proposed routing algorithm and five other routing algorithms listed before: CAODV, SEARCH, LAUNCH, AODV, and DORP.

**TABLE 3.** Simulation parameters (1).

| Parameter | Value |
|---|---|
| Channel Type | Channel/WirelessChannel |
| Radio propagation model | Propagation/FreeSpace |
| Network Interface Type | Phy/WirelessPhy |
| MAC Type | Mac/802.11e |
| Interface queue type | Queue/DropTail/PriQueue |
| Antenna Model | Antenna/OmniAntenna |
| Max. Packets in queue | 50 |
| # of mobile nodes | [0-100], [100-500] |
| Routing protocol | PERP |
| X- dimensions of topology | 100 |
| Y- dimensions of topology | 100 |
| # of channels/radio | 20 |
| Packet size | 512 bytes |
| Application | FTP |
| Percentage of malicious nodes | 5% of SUs |
| $\alpha$ | 0.3 |
| $\beta$ | 0.7 |
| $\mu$ | 0.5 |
| $\varepsilon$ | 0.3 |
| $\vartheta$ | 0.2 |

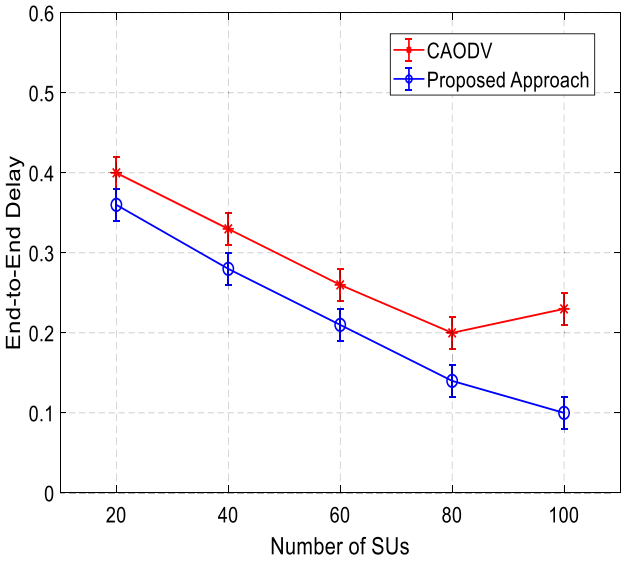


**FIGURE 3.** End-to-End Delay (Proposed Approach vs. COADV).

The comparison between the end-to-end delay in our proposed algorithm and CAODV is illustrated in Figure 3. It is depicted that the relation between the end-to-end delay and the number of SUs in the network is an inverse relation. In other words, as the number of SUs increase, the end-to-end delay decreases in both the approaches. However, in our proposed approach, it decreases more than that in CAODV; therefore, our proposed routing algorithm outperforms the CAODV routing algorithm. The end-to-end delay in our proposed routing algorithm is improved by up to 60% when the number of SUs is equal to 100. The reason that the end-to-end delay decreases with the increment of number of SUs is because having more SUs increases the chance of having more paths; therefore, the packets will be re-routed if one path is congested or unavailable.

**TABLE 4.** Simulation parameters(2).

| Parameter | Value |
|---|---|
| Channel Type | Channel/WirelessChannel |
| Radio propagation model | Propagation/FreeSpace |
| Network Interface Type | Phy/WirelessPhy |
| MAC Type | Mac/802.11e |
| Interface queue type | Queue/DropTail/PriQueue |
| Antenna Model | Antenna/OmniAntenna |
| Max. Packets in queue | 50 |
| Number of Nodes | 80 |
| Distribution Range | 200*200 square units |
| Transmission Range | 15 units |
| Number of channels | 6 |
| Percentage of malicious nodes | 5-60% |
| Packet size | 512 bytes |
| Application | FTP |
| Percentage of malicious nodes | 5% of SUs |
| $\alpha$ | 0.3 |
| $\beta$ | 0.7 |
| $\mu$ | 0.5 |
| $\varepsilon$ | 0.3 |
| $\vartheta$ | 0.2 |

Figure 4 illustrates the comparison between the end-to-end delay in our proposed approach and the two other routing algorithms, SEARCH and LAUNCH. As the relation between the number of SUs in the network and the end-to-end delay is inverse, incrementing the number of trusted SUs decreases the end-to-end delay since more nodes in the network increases the number of paths. Our proposed algorithm outperforms the other two routing approaches, as secure nodes forward packets to their next hop without delaying/dropping them. It is depicted in the figure that the end-to-end delay is improved by up to 41% and 74% as

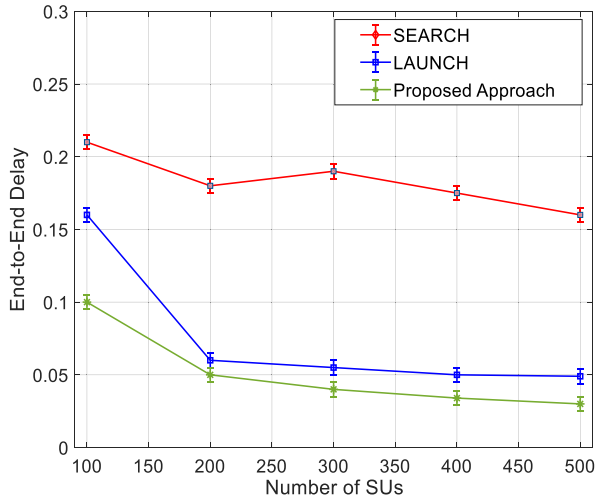


**FIGURE 4.** End-to-End Delay (Proposed Approach vs. SEARCH vs. LAUNCH).

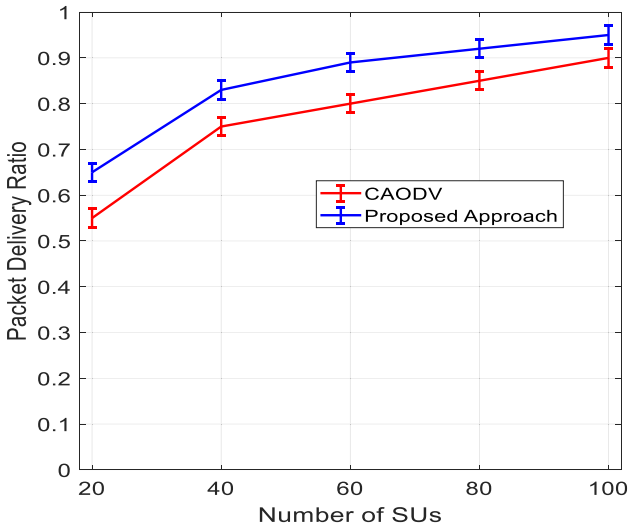


**FIGURE 5.** Packet Delivery Ratio (Proposed Approach vs. COADV).

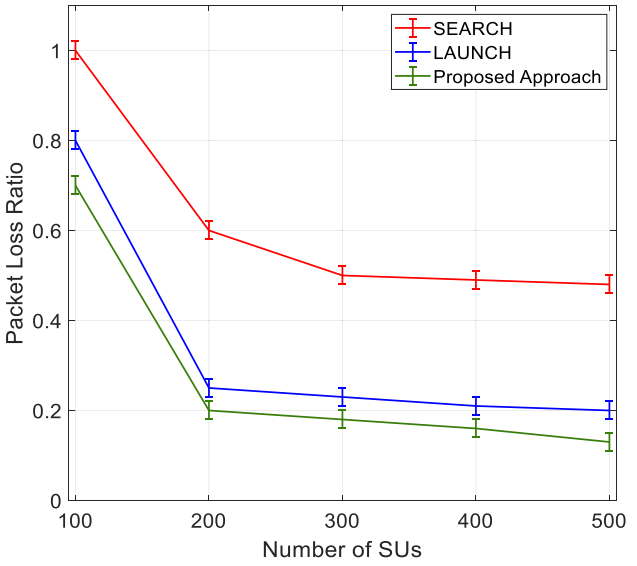


**FIGURE 6.** Packet Loss Ratio (Proposed Approach vs. SEARCH vs. LAUNCH).

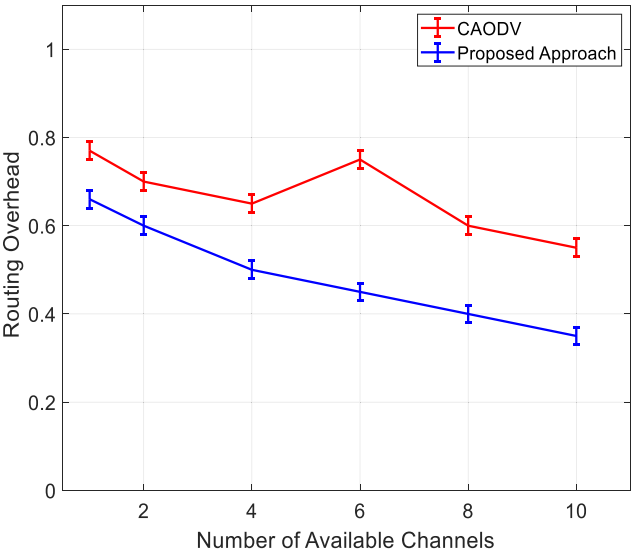


**FIGURE 7.** Routing Overhead (COADV vs. Proposed Approach).

compared with that in LAUNCH and SEARCH protocols, respectively.

In Figure 5, we have compared the packet delivery ratio in our proposed approach to the CAODV routing protocol. Moreover, the packet loss ratio in our proposed approach is compared with SEARCH and LAUNCH protocols, as illustrated in Figure 6. It is clear from Figure 5 that the relation between the packet delivery ratio and the number of SUs in the network is proportional. In other words, the packet delivery ratio increases with the increment of the number of trusted SUs in the network, as multiple routes exist. The packet delivery ratio reaches a higher value in our proposed routing algorithm. It can reach up to 95% using our proposed approach as compared with that in CAODV. On the other hand, Figure 6 illustrates the comparison between the packet loss ratio in our proposed routing algorithm and the two other routing algorithms, LAUNCH and SEARCH. In this simulation scenario, more SUs were implemented to measure the packet loss ratio, as well as the scalability of the three routing algorithms. It is depicted that the three routing algorithms are scalable and can work fine with higher number of SUs; however, our proposed routing algorithm performs better than LAUNCH and SEARCH. The packet loss ratio drops quickly when more trustworthy SUs take part in forwarding the packets over the network. For example, when the number of trusted SUs is equal to 100, the packet loss ratio is equal to 100%, 80%, and 70% in SEARCH, LAUNCH, and our proposed approach, respectively. Our proposed routing algorithm succeeds in obtaining the minimum packet loss ratio as compared with those in SEARCH and LAUNCH, which reveals that our proposed approach overtakes the SEARCH and LAUNCH routing algorithms.

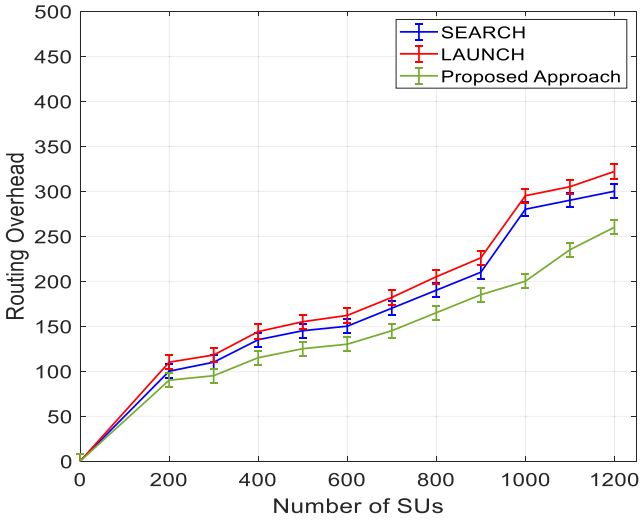


**FIGURE 8.** Routing Overhead (Proposed Approach vs. SEARCH vs. LAUNCH).

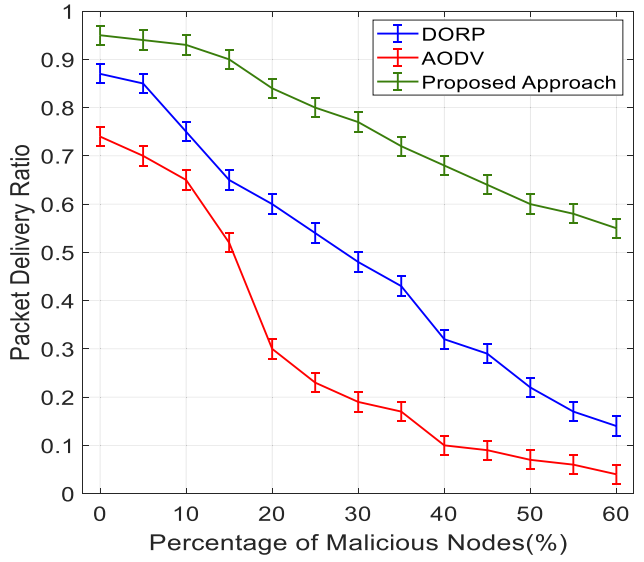


**FIGURE 9.** Packet Delivery Ratio (Proposed Approach vs. AODV vs.DORP).

The routing overhead in the proposed approach is compared to that in CAODV, SEARCH, and LAUNCH routing algorithms in Figures 7 and 8. In Figure 7, the routing overhead is measured as the ratio of the routing packets to the total number of packets sent over the network. It is illustrated that as the nodes have more channels for sending more routing requests, the routing overhead decreases when the number of available channels increase. Our proposed approach outperforms the CAODV and keeps the routing overhead at a minimum ratio as compared to that of CAODV. In Figure 8, the routing overhead is measured in terms of number of packets routed over the network. Despite the increment of routing overhead with the increase of the number of SUs, our proposed approach has a lower routing overhead as compared to that of SEARCH and LAUNCH routing algorithms.

Figure 9 compares our proposed approach with DORP and AODV in terms of the packet delivery ratio. It is clear

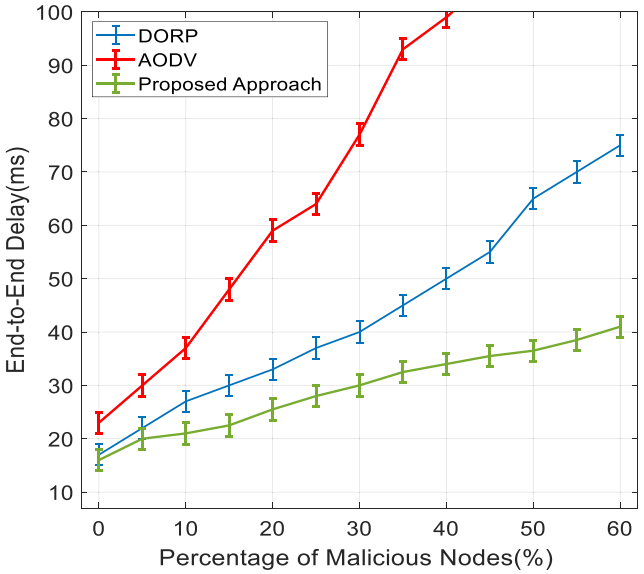


**FIGURE 10.** End-to-End Delay (Proposed Approach vs. AODV vs. DORP).

from the figure that the packet delivery ratio decreases when more malicious nodes are present in the network. However, the packet deliver ratio in the proposed approach is better than that of the DORP and AODV algorithms because the routes contain only normal-behaving nodes; nodes that have lower belief level are excluded. Our proposed approach achieves up to 11 times better packet delivery ratio than DORP and AODV algorithms when 60% of the network nodes misbehave.

Figure 10 compares our proposed approach with DORP and AODV in terms of the end-to-end delay. It is clear from the figure that the end-to-end delay increases when more malicious nodes are present in the network. However, the end-to-end delay in the proposed approach is better than that in DORP and AODV algorithms because the routes contain only normal-behaving nodes; and nodes that have lower belief level are excluded. Our proposed approach achieves up to 5 times less end-to-end delay than DORP and AODV algorithms when 60% of the network nodes misbehave.

In Table 5 and Table 6, we have compared our proposed approach to the COADV, LUANCH, SEARCH, DORP, and AODV routing algorithms in terms of the routing metrics used and the characteristics supported by the protocols. Table 5 summarizes the routing metrics used in the other routing protocols (SEARCH, LAUNCH, COADV, DORP, and AODV) as compared with our proposed approach. It is depicted that the different routing algorithms merge several routing metrics to accomplish various objectives of discovering the best routes; however, they did not think about security to be a routing metric. Therefore, their algorithms are vulnerable to attacks, and they do not properly work in case adversary nodes participate in routes establishment. On the other hand, our proposed solution uses security as a routing metric; thus, adversary nodes are identified and eliminated from participating in routes establishments. This behavior enhances the routes' reliability. In Table 6, we compare the different

**TABLE 5.** Different routing algorithms characteristics comparison (1).

| Routing Protocol/Metric | Delay | Spectrum Availability | Location-based | Security |
|---|---|---|---|---|
| **SEARCH** | Considered | Not Considered | Considered | Not Considered |
| **LAUNCH** | Considered | Not Considered | Considered | Not Considered |
| **COADV** | Not Considered | Considered | Not Considered | Not Considered |
| **DORP** | Considered | Not Considered | Not Considered | Not Considered |
| **AODV** | Not Considered | Not Considered | Considered | Not Considered |
| **Proposed Approach** | Considered | Considered | Considered | Considered |

**TABLE 6.** Different routing algorithms characteristics comparison (2).

| Routing Protocol/characteristic | Centralized/Distributed | Route Maintenance Support | Mobility Support | Common Control Channel | Secure Routes |
|---|---|---|---|---|---|
| **SEARCH** | Distributed | Considered | Considered | Not Considered | Not Considered |
| **LAUNCH** | Distributed | Considered | Considered | YES | Not Considered |
| **COADV** | Distributed | Considered | Considered | Not Considered | Not Considered |
| **DORP** | Distributed | Considered | Considered | Not Considered | Not Considered |
| **AODV** | Distributed | Considered | Considered | Not Considered | Not Considered |
| **Proposed Approach** | Distributed | Considered | Considered | Considered | Considered |

routing algorithms based on different characteristics that they can support. These characteristics are as follows:

- Centralized/Distributed: in central routing algorithms, best routes are found based on the different network nodes' information that is collected by a central node, whereas in distributed routing algorithms, the different network nodes participate in finding the best network routes.
- Route Maintenance Support: represents the ability of the routing algorithm of modifying the paths in case of PU presence over the currently used channels.
- Mobility Support: represents the ability of the routing algorithm of considering the mobility of Sus in the network.
- Common Control Channel: represents the routing algorithm requirement of having a predefined channel known to all network nodes, which is used to forward the routing packets.
- Secure Routes: shows if the different routes are secure, as well as if the security is considered in finding the best paths.

It is depicted from the tables below that most of the characteristics are supported by all the routing protocols support and on contrary they lack some of them; however, all of these characteristics are supported by the proposed approach. Therefore, the proposed approach is proven to be a better choice to be applied in CRNs.

### D. VERIFICATION THROUGH SCYTHER

We verified the correctness of our routing algorithm by using a well-known verification tool, namely Scyther [46]. Scyther is a verification tool that can check the existence of any attack that might negatively affect the correctness of the routing protocol. Scyther can detect the occurrence of many attacks such as man-in-the middle, sybil, PUEA, SSDF, and others. Figure 11 shows the verification process. Our routing algorithm is secure, and none of the aforementioned attacks can eavesdrop on messages sent between the reporting node and the CH. Moreover, the security level of the proposed approach can be depicted from the '' comments'' column that shows ''no attacks,'' which means that the sensing-reputation reports are sent and received safely by the reporting node and

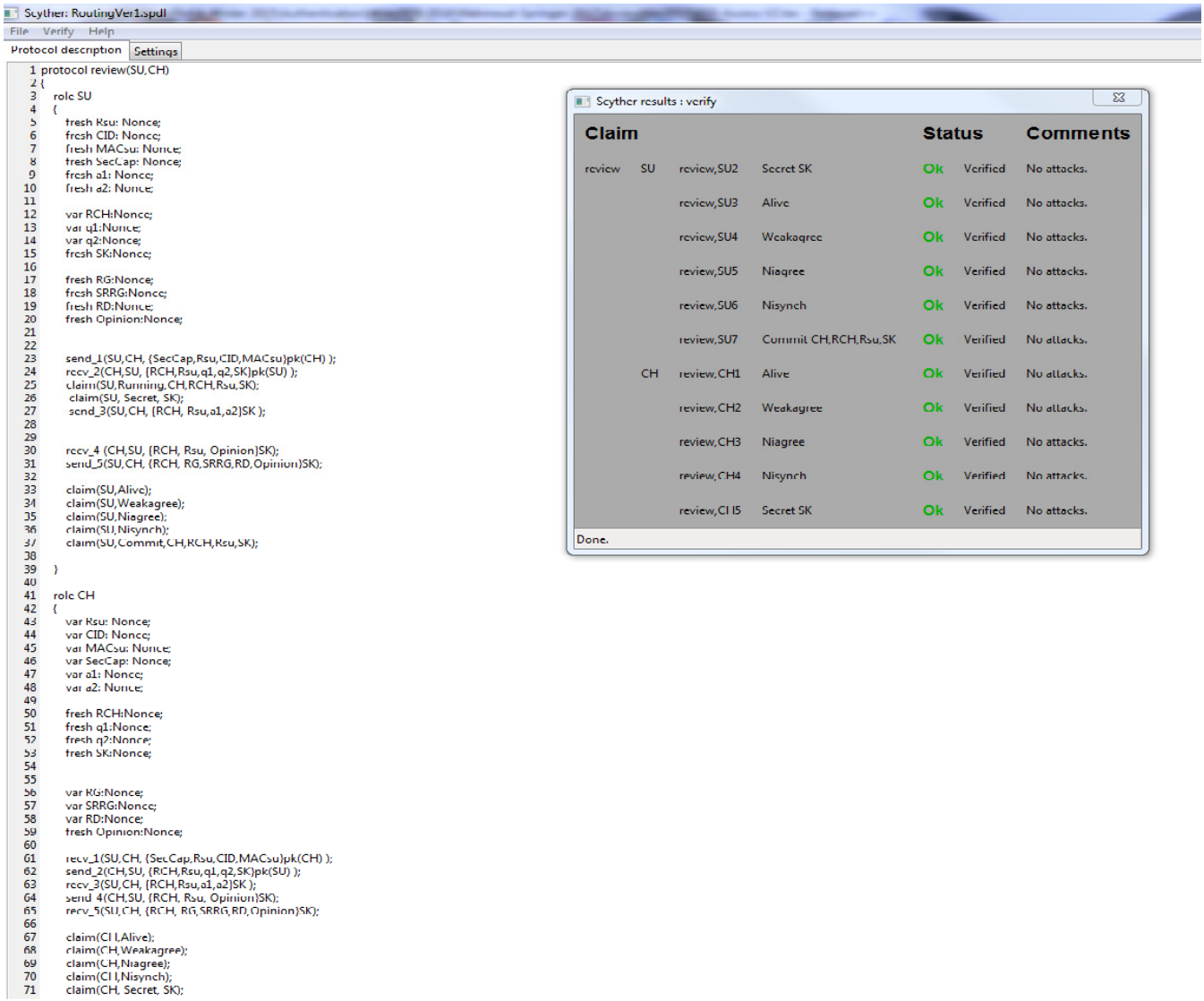


**FIGURE 11.** The Results of Verfiying the Proposed routing Algorithm in the Scyther Enviorment.

the CH repitively. Consequently, we are able to infer from the verification process applied to our proposed routing approach that the routing approach is ffective in improving the packet dilevery ratio with effectively no overhead on the CH. The repititive formal verification of the proposed routing algorithm provided useful insights of the routing algorithm during its developing time and helped in the approach development indeed.

## VI. CONCLUSION

Spectrum scarcity problem can be overcome with effective CR technology. Spectrum sensing is the initial important phase of exploiting unused spectrum bands. However, as the presence of adversary nodes can make the spectrum sensing results ineffective, investigating the reliability of sensing nodes becomes more important. Therefore, security of the sensing nodes must be taken into consideration before data is routed over the network. To build secure routing protocols/algorithms, the nodes' behavior during spectrum sensing is important and must be analyzed. Effective and secure routing algorithms enhance the network performance and increase network reliability. Current routing mechanisms in CRNS do not consider security to be a routing metric. They focus more on securing the routes of message exchange, which is important; however, counting security as a routing metric is more important to prevent malicious nodes from targeting the networks, thereby degrading the network performance. In this paper, we proposed a routing algorithm that combines the spectrum sensing and spectrum management phases. The routing algorithm uses security as a routing metric combined with other metrics relying on nodes' behavior during the spectrum sensing phase to manage the spectrum access. The proposed approach aims to find secure paths that consist of trusted sensing nodes only, which

enhances the network performance in terms of end-to-end delay, packet delivery /loss ratio, and routing overhead. The simulation results showed how the proposed approach outperformed other routing models. It improved the network performance measures, which increased the network security, and implicitly enhanced the spectrum utilization and the network throughput. As a future direction, the proposed approach can be used in IoT-constrained devices that can be used smaller networks for faster responses.

## REFERENCES

[1] J. Mitola, "Cognitive radio for flexible mobile multimedia communications," in *Proc. MoMuC*, 1999, pp. 3–10.
[2] W. Lee, "Resource allocation for multi-channel underlay cognitive radio network based on deep neural network," *IEEE Commun. Lett.*, vol. 22, no. 9, pp. 1942–1945, Sep. 2018.
[3] H. Anandakumar and K. Umamaheswari, "Cooperative spectrum handovers in cognitive radio networks," in *Proc. Cognit. Radio, Mobile Commun. Wireless Netw.* Cham, Switzerland: Springer, 2019, pp. 47–63.
[4] S. Mishra, S. S. Singh, and B. S. P. Mishra, "A comparative analysis of centralized and distributed spectrum sharing techniques in cognitive radio," in *Computational Intelligence in Sensor Networks*. Berlin, Germany: Springer, 2019, pp. 455–472.
[5] M. Khasawneh and A. Agarwal, "A secure routing algorithm based on nodes behavior during spectrum sensing in cognitive radio networks," in *Proc. IEEE 35th Int. Perform. Comput. Commun. Conf. (IPCCC)*, Las Vegas, NV, USA, Dec. 2016, pp. 1–8, doi: 10.1109/PCCC.2016.7820642.
[6] M. Khasawneh, "A hierarchical structure towards securing data transmission in cognitive radio networks," Ph.D. dissertation, Dept. Elect. Comput. Eng., Concordia Univ., Montreal, QC, Canada, 2017.
[7] C. Liu and L. Xiao, "Building $\kappa$-protected routes in multi-hop cognitive radio networks," *IEEE Trans. Cognit. Commun. Netw.*, vol. 5, no. 4, pp. 976–989, Dec. 2019, doi: 10.1109/TCCN.2019.2932389.
[8] F. Hu, B. Chen, and K. Zhu, "Full spectrum sharing in cognitive radio networks toward 5G: A survey," *IEEE Access*, vol. 6, pp. 15754–15776, 2018.
[9] J. Wang, H. Yue, L. Hai, and Y. Fang, "Spectrum-aware anypath routing in multi-hop cognitive radio networks," *IEEE Trans. Mobile Comput.*, vol. 16, no. 4, pp. 1176–1187, Apr. 2017.
[10] H. Ma, L. Zheng, X. Ma, and Y. Luo, "Spectrum aware routing for multi-hop cognitive radio networks with a single transceiver," in *Proc. 3rd Int. Conf. Cognit. Radio Oriented Wireless Netw. Commun. (CrownCom)*, May 2008, pp. 1–6.
[11] F. Tang, C. Tang, Y. Yang, L. T. Yang, T. Zhou, J. Li, and M. Guo, "Delay-minimized routing in mobile cognitive networks for time-critical applications," *IEEE Trans. Ind. Informat.*, vol. 13, no. 3, pp. 1398–1409, Jun. 2017.
[12] G. Cheng, W. Liu, Y. Li, and W. Cheng, "Joint on-demand routing and spectrum assignment in cognitive radio networks," in *Proc. IEEE Int. Conf. Commun.*, Jun. 2007, pp. 6499–6503.
[13] Z. Yang, G. Cheng, W. Liu, W. Yuan, and W. Cheng, "Local coordination based routing and spectrum assignment in multi-hop cognitive radio networks," *Mobile Netw. Appl.*, vol. 13, nos. 1–2, pp. 67–81, Apr. 2008.
[14] K. R. Chowdhury and M. D. Felice, "Search: A routing protocol for mobile cognitive radio ad-hoc networks," *Comput. Commun.*, vol. 32, no. 18, pp. 1983–1997, Dec. 2009.
[15] S.-C. Lin and K.-C. Chen, "Spectrum aware opportunistic routing in cognitive radio networks," in *Proc. IEEE Global Telecommun. Conf. (GLOBECOM)*, Dec. 2010, pp. 1–6.
[16] Y. Liu, L. X. Cai, and X. S. Shen, "Spectrum-aware opportunistic routing in multi-hop cognitive radio networks," *IEEE J. Sel. Areas Commun.*, vol. 30, no. 10, pp. 1958–1968, Nov. 2012.
[17] C. E. Perkins and E. M. Royer, "Ad-hoc on-demand distance vector routing," in *Proc. 2nd IEEE Workshop Mobile Comput. Syst. Appl.*, New Orleans, LA, USA, 1990, pp. 90–100.
[18] A. S. Cacciapuoti, M. Caleffi, and L. Paura, "Reactive routing for mobile cognitive radio ad hoc networks," *Ad Hoc Netw.*, vol. 10, no. 5, pp. 803–815, Jul. 2012.
[19] I. Pefkianakis, S. H. Y. Wong, and S. Lu, "SAMER: Spectrum aware mesh routing in cognitive radio networks," in *Proc. 3rd IEEE Symp. New Frontiers Dyn. Spectr. Access Netw.*, Oct. 2008, pp. 1–5.
[20] S.-J. Lee and M. Gerla, "Split multipath routing with maximally disjoint paths in ad hoc networks," in *Proc. IEEE Int. Conf. Commun. Conf. Rec. (ICC)*, vol. 10, Jun. 2002, pp. 3201–3205.
[21] X. Li and L. Cuthbert, "On-demand node-disjoint multipath routing in wireless ad hoc networks," in *Proc. 29th Annu. IEEE Int. Conf. Local Comput. Netw.*, Nov. 2004, pp. 419–420.
[22] Y. Le, X. Cheng, D. Chen, N. Zhang, T. Znati, M. A. Al-Rodhaan, and A. Al-Dhelaan, "Distributed back-pressure scheduling with opportunistic routing in cognitive radio networks," *EURASIP J. Wireless Commun. Netw.*, vol. 2015, no. 1, pp. 1–14, Dec. 2015.
[23] C.-J. Chae and H.-J. Cho, "Enhanced secure device authentication algorithm in P2P-based smart farm system," *Peer Peer Netw. Appl.*, vol. 11, no. 6, pp. 1230–1239, Nov. 2018.
[24] K. Fan, J. Wang, X. Wang, H. Li, and Y. Yang, "Secure, efficient and revocable data sharing scheme for vehicular fogs," *Peer Peer Netw. Appl.*, vol. 11, no. 4, pp. 766–777, Jul. 2018.
[25] F. Tang, L. Barolli, and J. Li, "A joint design for distributed stable routing and channel assignment over multihop and multiflow mobile ad hoc cognitive networks," *IEEE Trans. Ind. Informat.*, vol. 10, no. 2, pp. 1606–1615, May 2014.
[26] X. He, H. Jiang, Y. Song, C. He, and H. Xiao, "Routing selection with reinforcement learning for energy harvesting multi-hop CRN," *IEEE Access*, vol. 7, pp. 54435–54448, 2019, doi: 10.1109/ACCESS.2019.2912996.
[27] K. Habak, M. Abdelatif, H. Hagrass, K. Rizc, and M. Youssef, "A location-aided routing protocol for cognitive radio networks," in *Proc. Int. Conf. Comput., Netw. Commun. (ICNC)*, Jan. 2013, pp. 729–733.
[28] K.-W. Chin, L. Wang, and S. Soh, "Joint routing and links scheduling in two-tier multi-hop RF-energy harvesting networks," *IEEE Commun. Lett.*, vol. 20, no. 9, pp. 1864–1867, Sep. 2016.
[29] P.-D. Thanh, H. Vu-Van, and I. Koo, "Efficient channel selection and routing algorithm for multihop, multichannel cognitive radio networks with energy harvesting under jamming attacks," *Secur. Commun. Netw.*, vol. 2018, Mar. 2018, Art. no. 7543212, doi: 10.1155/2018/7543212.
[30] A. Banerjee, A. Paul, and S. P. Maity, "Joint power allocation and route selection for outage minimization in multihop cognitive radio networks with energy harvesting," *IEEE Trans. Cognit. Commun. Netw.*, vol. 4, no. 1, pp. 82–92, Mar. 2018.
[31] X. Ding, Y. Zou, G. Zhang, X. Chen, X. Wang, and L. Hanzo, "The security–reliability tradeoff of multiuser scheduling-aided energy harvesting cognitive radio networks," *IEEE Trans. Commun.*, vol. 67, no. 6, pp. 3890–3904, Jun. 2019.
[32] E. Barka, C. Kerrache, H. Benkraouda, K. Shuaib, F. Ahmad, and F. Kurugollu, "Towards a trusted unmanned aerial system using blockchain for the protection of critical infrastructure," *Trans. Emerg. Telecommun. Technol.*, p. e3706, Jul. 2019. [Online]. Available: https://onlinelibrary.wiley.com/toc/21613915/0/0
[33] G. Rathee, H. Saini, and G. Singh, "Aspects of trusted routing communication in smart networks," *Wireless Pers. Commun.*, vol. 98, no. 2, pp. 2367–2387, Jan. 2018.
[34] F. Ahmad, V. N. L. Franqueira, and A. Adnane, "TEAM: A trust evaluation and management framework in context-enabled vehicular ad-hoc networks," *IEEE Access*, vol. 6, pp. 28643–28660, 2018.
[35] M. Sharifi, A. A. Sharifi, and M. J. M. Niya, "Cooperative spectrum sensing in the presence of primary user emulation attack in cognitive radio network: Multi-level hypotheses test approach," *Wireless Netw.*, vol. 24, no. 1, pp. 61–68, Jan. 2018.
[36] C. Zhu, J. J. P. C. Rodrigues, V. C. M. Leung, L. Shu, and L. T. Yang, "Trust-based communication for the industrial Internet of Things," *IEEE Commun. Mag.*, vol. 56, no. 2, pp. 16–22, Feb. 2018.
[37] E. P. K. Gilbert, B. Kaliaperumal, E. B. Rajsingh, and M. Lydia, "Trust based data prediction, aggregation and reconstruction using compressed sensing for clustered wireless sensor networks," *Comput. Electr. Eng.*, vol. 72, pp. 894–909, Nov. 2018.
[38] D. Xu, S. Zhang, J. Chen, and M. Ma, "A provably secure anonymous mutual authentication scheme with key agreement for SIP using ECC," *Peer Peer Netw. Appl.*, vol. 11, no. 5, pp. 837–847, Sep. 2018.
[39] M. Zheng, C. Wang, M. Du, L. Chen, W. Liang, and H. Yu, "A short preamble cognitive MAC protocol in cognitive radio sensor networks," *IEEE Sensors J.*, vol. 19, no. 15, pp. 6530–6538, Aug. 2019.
[40] K.-L.-A. Yau, N. Ramli, W. Hashim, and H. Mohamad, "Clustering algorithms for cognitive radio networks: A survey," *J. Netw. Comput. Appl.*, vol. 45, pp. 79–95, Oct. 2014.

[41] M. Khasawneh and A. Agarwal, "A secure and efficient authentication mechanism applied to cognitive radio networks," *IEEE Access*, vol. 5, pp. 15597–15608, 2017, doi: 10.1109/ACCESS.2017.2723322.
[42] M. Khasawneh and A. Agarwal, "A collaborative approach for monitoring nodes behavior during spectrum sensing to mitigate multiple attacks in cognitive radio networks," *Secur. Commun. Netw.*, vol. 2017, pp. 1–16, Jan. 2017, doi: 10.1155/2017/3261058.
[43] M. Khasawneh, A. Agarwal, N. Goel, M. Zaman, and S. Alrabaee, "Sureness efficient energy technique for cooperative spectrum sensing in cognitive radios," in *Proc. Int. Conf. Telecommun. Multimedia (TEMU)*, Heraklion, Greece, Jul. 2012, pp. 25–30.
[44] A. R. Kulkarni and A. Agarwal, "Energy-efficient QoS based route management in cognitive radio networks," in *Proc. IEEE Int. Conf. Data Sci. Data Intensive Syst.*, Dec. 2015, pp. 304–310.
[45] M. Khasawneh and A. Agarwal, "A collaborative approach towards securing spectrum sensing in cognitive radio networks," in *Proc. 11th Int. Conf. Future Netw. Commun. (FNC), Procedia Comput. Sci.*, 2016, pp. 302–309.
[46] C. Cremers. *Scyther Tool*. Accessed: Mar. 27, 2020. [Online]. Available: https://people.cispa.io/cas.cremers/scyther/

**MAHMOUD KHASAWNEH** (Member, IEEE) received the M.Sc. and Ph.D. degrees in electrical and computer engineering from Concordia University, Canada, in 2012 and 2017, respectively. He is currently an Assistant Professor with the Department of Computer Engineering, American University of the Middle East, Kuwait. He has published many journal papers, conference papers, and a book chapter. He serves as a TPC in many prestigious conferences and a peer reviewer in different refereed journals in the field of computer science and engineering. His current research is in the various aspects of wireless networks, including security, authentication, and route management.

**AHMAD AZAB** (Member, IEEE) received the Ph.D. degree in information technology from the School of Science, Information Technology and Engineering, Federation University of Australia. He is currently an Assistant Professor with the Computer Engineering Department, College of Engineering, American University of Middle East (AUM), Kuwait. He works closely with academia and industry on many projects. His research interests include cybersecurity, network analysis, artificial intelligence, and digital forensics. He has published journal and conference papers within the area of his research interest. He has more than 10 years of both academic and industrial experience and worked on planning, implementing, and auditing cybersecurity solutions for various projects in Australia and the Middle East.

**ANJALI AGARWAL** (Senior Member, IEEE) received the B.E. degree in electronics and communication engineering from the Delhi College of Engineering, India, in 1983, the M.Sc. degree in electrical engineering from the University of Calgary, Alberta, in 1986, and the Ph.D. degree in electrical engineering from Concordia University, Montreal, in 1996. She is currently a Professor with the Department of Electrical and Computer Engineering, Concordia University, Montreal. Prior to joining faculty in Concordia, she has worked as a Lecturer in IIT Roorkee, and as a Protocol Design Engineer and a Software Engineer in industry. Her current research interests are in the various aspects of wireless networks, including security and virtualization of cognitive radio networks, resource management, heterogeneous networks, and cloud networks.