ITUJournal
Future and evolving technologies

ITU Journal on Future and Evolving Technologies, Volume 5, Issue 4, December 2024

ARTICLE

Digital Signature-based Authentication Framework in Cognitive Radio-Internet of Vehicles

Mohammad Amzad Hossain[1], Md. Sipon Miah[2,3,4], Ana Garcia Armada[3]

[1] Department of Information and Communication Engineering, Noakhali Science and Technology University, Noakhali, 3814, Bangladesh., [2] Department of Information and Communication Technology, Islamic University, Kushtia, 7003, Bangladesh., [3] Department of Signal Theory and Communications, Universidad Carlos III of Madrid, Leganes, Madrid, 28911, Spain., [4] Wireless Communications with Machine Learning (WCML) Laboratory, Islamic University, Kushtia, 7003, Bangladesh.

Corresponding author: Md. Sipon Miah, mmiah@ing.uc3m.es

The Internet of Vehicles (IoV) is an evolution of the Internet of Things (IoT). IoV allows real-time information-sharing of intra-vehicle, inter-vehicle and vehicle to the roadside base stations, which improves transport safety and reduces road traffic accidents. Due to the increased number of vehicles in IoV networks, the allocated spectrum bands are not sufficient for a large number of vehicles. Cognitive Radio-enabled IoV (CR-IoV) is a novel concept that mitigates the spectrum shortage problem by allowing unlicensed user access to the licensed user spectrum in convenient conditions. Due to the dynamic spectrum sharing feature of CR-IoV, a Malicious User (MU) can easily perform an attack in the network at any time. To mitigate this problem, we propose a digital signature-based authentication framework secure cooperative spectrum sensing technique for detecting the MU in the CR-IoV network. In this paper, the proposed framework ensures the integrity, authenticity, and non-repudiation of messages exchanged between vehicles and CR-enabled base stations. The framework is designed to detect and mitigate security threats such as impersonation, data tampering, and unauthorized access, which are prevalent in CR-IoV networks. Furthermore, the proposed solution addresses the Dynamic Spectrum Access (DSA) vulnerability by integrating cryptographic mechanisms into the cognitive radio process, ensuring secure spectrum handovers and minimizing the risk of malicious attacks during spectrum sensing and sharing. Simulation results show that the proposed digital signature-based authentication framework provides 100% correct detection and 0% mis-detection rate for both legitimate users and malicious users in the CR-IoV networks. Therefore, the proposed scheme significantly enhances sensing gain and communication security while maintaining lower global error probability and overhead than other existing frameworks, making it highly suitable for real-time vehicular applications. Moreover, this proposed scheme plays a pivotal role in advancing secure vehicular communications, thereby contributing to the development of safer and more reliable intelligent transportation systems.

Keywords: Cognitive radio-Internet of Vehicles, digital signature, legitimate user, malicious user

1. INTRODUCTION

Day-by-day the Internet of Things (IoT) is becoming the backbone of all wireless communication systems that will host a huge number of communication devices to share data with each other intelligently [1, 2]. Nowadays, existing transport systems are being transformed into Intelligent Transportation System (ITS) by embedding IoT facilities [3, 4]. Moreover, Cooperative ITS (C-ITS) aims to make strides in improving the safety and manageability of land transportation and reducing road congestion, through a suite of communications and platforms for data delivery [5]. The Internet of Vehicles (IoV) is a conversion of Vehicular Ad hoc Networks (VANETs), which enables vehicles to use the Internet for exchanging information between Vehicle-to-Vehicle (V2V), Vehicle-to-Infrastructure (V2I), Vehicle-to-Pedestrian (V2P), Vehicle-to-Roadside (V2R) and

Vehicle-to-Everything (V2X) [6]. However, the growth of IoV networks is hampered by several problems such as the fact that it requires greater bandwidth to connect a large number of vehicles and applications, and maintaining secure data sharing across heterogeneous devices [7].

IEEE 802.11p dedicated short-range communications Wireless Access in Vehicular Environments (WAVE) standard used for wireless vehicular communications consists of one control channel used for establishing connection and only 6 channels that are allocated for vehicular data [8]. Morever, the U.S. Federal Communications Commission (FCC) has allocated only 75 MHz of spectrum in the 5.9 GHz band for the implementation of ITS services in the VANETs, which is not enough for a large number of vehicles [9, 5]. Cognitive Radio (CR) is a novel concept to alleviate the spectrum shortage issue by permitting the Secondary User (SU) to use the allocated spectrum of the Primary User (PU) when the spectrum is idle [10]. In a cognitive Radio enabled IoV (CR-IoV) network, each vehicle is opportunistically accessing the idle PU's spectrum when the PU is inactive in the network [11].

The most important aspect of the CR-IoV network is spectrum sensing to resolve damaging interference between the licensed user and CR-embedded Vehicles (CRV) [12]. One of the most commonly used methods of licensed spectrum detection is the Energy Detection (ED) method; it is fast and requires no prior understanding of the PU signal [13]. However, the sensing accuracy of the ED method is reduced for several issues such as the channel fading and the hidden node problem [14]. The CSS approach was explored to resolve the problems of energy detection-based spectrum detection [15, 16].

Security is another vital issue for CR-IoV networks due to the fact that heterogeneous wireless devices are permitted to use the licensed spectrum also used the CR-IoV networks are vulnerable to attack of Malicious Users (MUs) resulting in an increase of the spectrum demand, decrease of the quality of service, data security, and reliability [17, 18]. Therefore, nowadays the issues of licensed spectrum access security in the CR-IoV networks have become an important research topic. In [19], the authors proposed a centralized Cooperative Spectrum Sensing (CSS) approach which enhances the spectrum detection gain at a Fusion Center (FC). The authors examined the probabilities of detection and false alarm only. However, they did not consider the security issue, the throughput and the global error probability.

In [20], the authors introduced a double adaptive threshold concept to differentiate the Legitimate Users (LUs) and MUs based on the weight of each user so that the LU weight is higher then the MU. However, each user weight is calculated by using the Maximal Ratio Combining (MRC) rule which increases the calculation time, a reason why it is not suitable for CR-IoV networks. In [21], the authors used the Support Vector Machine (SVM) for detecting a malicious primary user signal based on the Signal-to-Noise Ratio (SNR) values and entropy of the received PU signal. However, the SNR value and entropy calculation of the received signal at the Fusion Center (FC) increased execution complexity, and time. Moreover, the MUs detection accuracy of the SVM is not sufficient to prevent MU attacks on the CR-IoV network.

In [22], the authors proposed a secure enhanced non-cooperative cognitive division multiple access for Vehicle-to-Vehicle (V2V) communication where the message integrity and privacy were preserved using the commutative RSA cryptography technique. In [23], the authors proposed a secure privacy-preserving authentication scheme for Vehicular Ad-hoc Networks (VANETs) with Cuckoo filter. In [24], the authors proposed a blockchain-based method for MU detection in networks where this strategy makes it simple to distinguish between a trustworthy user and a MU using cryptography keys. In [25], the authors explained different types of attacks in a Cognitive Radio Ad-hoc Vehicular Network (CRAVENET). In [26], the authors proposed a digital signature-based trust-oriented scheme to ensure communication by identifying efficient trustworthy users in CRNs.

In [27], the authors introduced blockchain-based MU identification with SHA-3 hashing and and ED-based Spectrum sensing approach. The proposed approach achieves 3.125%, 6.5% and 8.8% more detection probability at -5 dB SNR in the presence of a MU, when compared to other methods like Equal Gain Combining (EGC), Blockchain-based Cooperative Spectrum Sensing (BCSS) and Fault Tolerant Cooperative Spectrum Sensing (FTCSS) respectively. However, the authors did not consider the mobility of the cognitive radio user for the simulation results.

In [28], the authors proposed a blockchain-based scheme to detect the malevolent user in the CRN by using an adaptive threshold spectrum energy detection algorithm. The performance of this proposed approach is evaluated by metrics such as the probability of detection, false alarm probability, sensing performance gain, total error probability, missed detection probability, number of selected sensing nodes, average network throughput, and energy efficiency.

In view of the above, we propose a digital signature-based robust cooperative spectrum sensing scheme for enhancing the MUs' detection accuracy and minimizing the complexity in IoV networks. The proposed scheme is more secure and faster than previous solutions reported in the literature.

The key results of this article are given as follows:

- We propose a digital signature-based authentication framework for cooperative spectrum sensing in the CR-IoV network.
- Our simulation outcomes reveal that the proposed authentication framework correctly detects the MU and LU, enhancing sensing performance over the conventional scheme. Moreover, it decreases the global error probability at the FC over the conventional scheme.

The rest of this article is presented as follows. Section 2 describes the system model. In Section 3 we present our proposed authentication framework. The experimental results and conclusion are detailed in Section 4 and Section 5, respectively.

2. SYSTEM MODEL

In this section, we briefly explain the network structure, DoS attacks in CRNs, the ED technique, and the digital signature architecture.

2.1 Network structure

We propose a digital signature-based secure CSS scheme for CR-IoV networks which consist of N legitimate CRVs and M malicious users. In our model, each legitimate CRV senses the PU signal status and transmits their sensing data to the corresponding FC and at the same time malicious users forward their false sensing results to the FC. The FC uses the digital signature mechanism for detecting the legitimate user and the malicious user according to the public key and private key concept. Thereafter, the FC uses K-out-of-N fusion rule to take a global decision about the status of the PU signal. At the FC, our proposed authentication framework blocks the MU and enhances the detection probability of the PU signal status with respect to the conventional CSS technique.

We consider that PUs are static in our system model and CRVs are both static and mobile. To avoid interference between the PU signal and the CRV signal we need accurate identification of the PU signal status within a certain time and position. In the CR-IoV network, if PU is idle this condition is represented by $P_0 = OFF$ and if PU is active this condition is represented by $P_1 = ON$. The duration of the $P_0 = OFF$ and $P_1 = ON$ conditions are represented by the random parameters A and B, respectively. The parameters A and B follow exponential distributions with the average time D_A and D_B, respectively. The probabilities that PU is idle and active are defined as $P_0 = D_B/(D_A + D_B)$ and $P_1 = D_A/(D_A + D_B)$, respectively.

There are two states of the PU signal in the CR-IoV networks. These two states are represented by two hypotheses which are given as below:

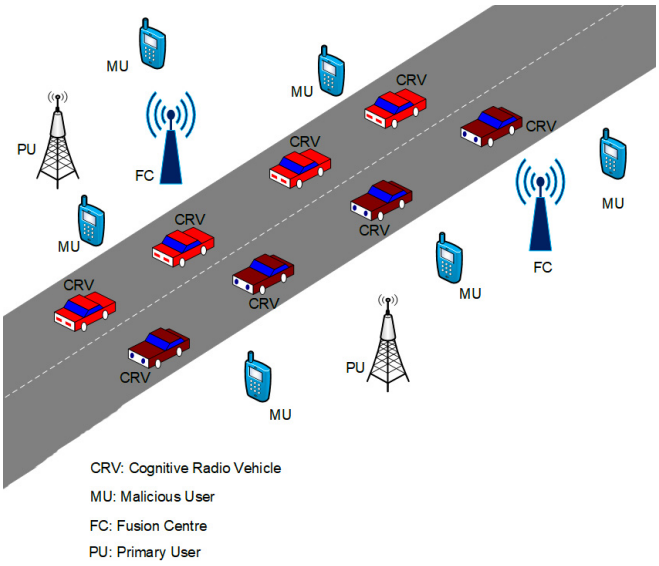

Figure 1 – The proposed network model.

$$\begin{cases} H_0: & \text{if the PU's signal is absent,} \\ H_1: & \text{if the PU's signal is present.} \end{cases} \quad (1)$$

The received signal at the ith CRV is represented for the two hypotheses as [29]:

$$y_i(l) = \begin{cases} n_i(l) & : H_0 \\ \theta_i(l)\, x(l) + n_i(l) & : H_1 \end{cases} \quad (2)$$

where $y_i(l)$, $x(l)$, $n_i(l)$ $\theta_i(l)$ are the received signal, the PU signal, an AWGN noise signal and antenna gain at the ith CRV, respectively. Moreover, l indicates the l^{th} sample in time.

2.2 Distributed Denial-of-Service (DDoS) in cognitive radio networks

In this paper, we considered polymorphic adversarial Distributed Denial-of-Service (DDoS) attacks. This type of malicious user changes the attack profile over time. A DDoS attack is an attack in which a malicious actor aims to reduce a legitimate user's bandwidth, prevent access to a service, or disrupt service to a specific system or a user. DDoS attacks accomplish this by flooding the target with traffic, or sending them information that triggers a crash. Cognitive radio networks, as special wireless communication networks, are vulnerable to DDoS attacks [30, 31, 32].

In cognitive radio networks, spectrum sensing technology is used to identify the presence of primary users and abandon the frequency band as quickly as possible if the corresponding primary user emerges in order to avoid

interference between CR-IoV users and primary users. Due to the introduction of spectrum sensing, two kinds of new denial of service attacks in the physical layer may be launched. Firstly, selfish secondary user or malicious secondary user launches Primary User Emulation (PUE) [33, 34] attack to prevent other legal CR-IoV users from using the idle spectrum band. Secondly, attackers may launch the mask primary user attack to prevent the primary users from using the licensed spectrum band.

2.3 Energy detection technique

The ED process is a more suitable technique to calculate the energy level of the received PU signal, because it can calculate the energy level without any prior information about the PU signal and with less time complexity than other techniques. [35]. The energy calculation process at the CRV is shown in Fig. 2.

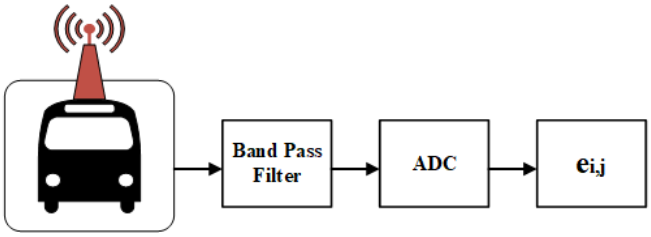

Figure 2 – The process of energy level calculation in ED technique.

The energy level of the received PU signal at the i^{th} CRV is calculated as follows [35]:

$$E_i = \sum_{l=1}^{L} |y_i(l)|^2 \qquad (3)$$

where L indicates the number of received samples.

2.4 Digital signature architecture

Digital signature is a decentralised networking architecture that ensures the secure data communications over the Internet. Nowadays digital signatures are embedded with several applications like IoT, wireless sensor networks, cloud computing, cryptocurrencies, and others [36]. Primarily the Digital Signature Algorithm (DSA) is developed to secure transmission of electronic financial transactions, exchange the data, distribution of software over the Internet and others, by using a digital signature mechanism to prove the authenticity [37].

Digital signature is an implementation of the concept of a public key and private key cryptography for secure data transfer [17]. It is a way to confirm that a message originated from a particular device and from no one else, like a malicious user or hacker [38]. The digitally signed message is broadcast over the entire network. There are two stages to the digital signature: the signing stage and the verification stage. Fig. 3 shows the architectural view of the digital signature.

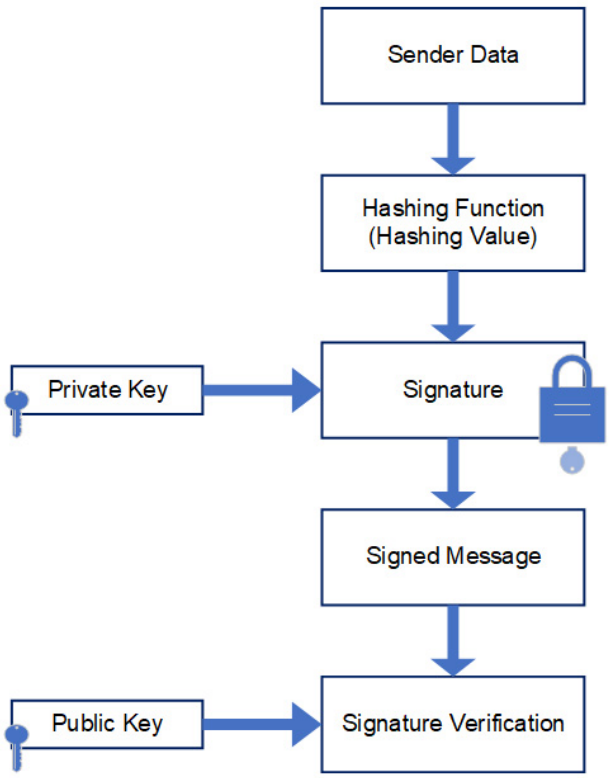

Figure 3 – Digital signature architecture.

Each signature contains the following elements [39]:

- Sender data: It contains the sender message intended for the receiver.
- Hashing value: The sender message is changed by hash function. The output of a hash function is called hashing value.
- Private key: The private key is a secure key that only the sender knows. It is used for creating digital signatures.
- Public key: The public key is an open key that everyone in the network knows. It is used by the receiver to verify the digital signature.

3. PROPOSED DIGITAL SIGNATURE-BASED AUTHENTICATION FRAMEWORK

In cognitive radio-based IoV networks, the primary users share their licensed spectrum with cognitive radio-enabled vehicles. It is a critical and important issue to ensure secure licensed spectrum sharing in CR-IoV networks. However, the CR-IoV networks are vulnerable to security attacks from both local and outside malicious users. The malicious user connects to the network and uses free licensed spectrum from PUs, which reduces the

chances of a legitimate user getting a free licensed spectrum from PUs for data communications. To improve authentication, integrity and secure licensed spectrum sharing in the CR-IoV networks, we proposed a digital signature-based authentication framework. Fig. 4 shows the schematic diagram of the proposed authentication framework for the CR-IoV networks.

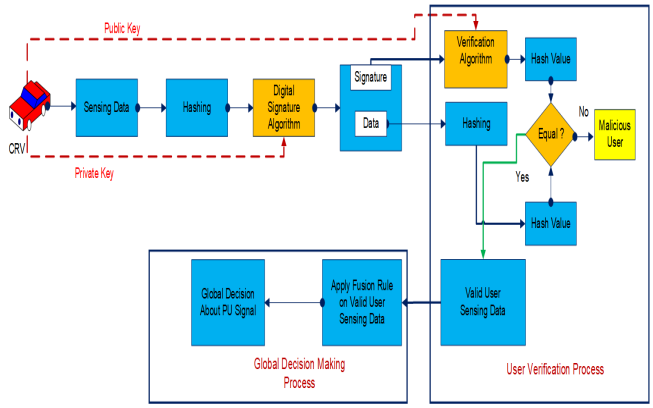

Figure 4 – The schematic diagram of the proposed digital signature-based authentication framework for CSS scheme.

In the proposed scheme, each CRV continuously senses the status of the PU signal in the CR-IoV networks. Thereafter, it encrypts their sensing data using a digital signature algorithm with a private key and transmits it to the FC through reporting channels. The FC verifies the authenticity of the sender i.e., CRV by using a verification algorithm with a public key. If the sender i.e., CRV is a legitimate user, this spectrum sensing data is forwarded into a global decision-making unit; on the other hand, if the sender is a malicious user, this spectrum sensing data is discarded. In a specific time interval, all sensing data is received from the legitimate CRVs.

Finally, the FC uses the "K-out-of-N rule" on all valid received test statistical data to make a global decision about the status i.e., active or inactive of the PU signal in the CR-IoV networks.

3.1 Verification process

There are two users in our proposed scheme, namely CRV is a signer, FC is a versifier. There are three important steps for the digital signature algorithm, such as key-pair generation, signature-generation and signature-verification [40].

DSA pey-pair generation:

1. Select a prime number α with Υ bit length ($512 \leq \Upsilon \leq 1024$). It is a public parameter.
2. Select another prime number β with length 160 bits, where $((\alpha - 1)\ mod\ \beta)$=0. It is a public parameter.
3. Compute $g = (h^{\frac{(\alpha-1)}{\beta}}\ mod\ \alpha)$, where $h < \alpha - 1$ and $(h^{\frac{(\alpha-1)}{\beta}}\ mod\ \alpha) > 1$. It is a public parameter.
4. ψ is a private key, where $\psi < q$.
5. φ is a public key, where $\varphi = (g^{\psi}\ mod\ \alpha)$.
6. m represents the sensing message that is to be signed.

Signature generation for message m: The CRV uses the digital signature algorithm to create a signature as follows:

1. Compute $r = (g^k \bmod \alpha)\ mod\ \beta$ where k represents a random integer value in the range $0 < k < \beta$.
2. Compute $s = (k^{-1}(SHA - 1(m) + \psi \times r))\ mod\ \beta$, where $SHA - 1(m)$ indicates the hash function.
3. (r, s) represents the digital signature. It is signed by the user private key ψ.

Signature verification process: To verify the digital signature (r, s), the FC uses a verification algorithm as follows:

1. Compute $z = (s)^{-1}\ mod\ \beta$.
2. Compute $t1 = (SHA - 1(m) \times z)\ mod\ \beta$.
3. Compute $t2 = (r \times z)\ mod\ \beta$.
4. Compute $c = ((g^{t1} \times \varphi^{t2})\ mod\ \alpha)\ mod\ \beta$.
5. If $c = r$ then the digital signature is valid and sender (i.e., CRV) is a legitimate user otherwise sender is a malicious user.

The proposed framework for implementing cryptography keys for authentication in the IoV must address several key challenges related to key management, distribution, and renewal, given the highly mobile and distributed nature of IoV. Here is how these challenges can be addressed.

Key management: Our proposed framework uses a decentralized key management approach where keys are managed locally by individual vehicles and regional authorities. This increases robustness, scalability and security.

Key distribution: Our proposed framework uses secure distribution channels for key distribution where secure channels such as Vehicle-to-Infrastructure (V2I) communications are utilized for key distribution, ensuring that only authenticated vehicles receive the keys.

Key renewal: Our proposed framework uses an automated key renewal scheme that triggers key updates at regular intervals or based on specific events (e.g., expiry, detection of a compromise).

By addressing these aspects, the proposed framework can effectively manage cryptographic keys in a highly mobile and distributed IoV environment, ensuring secure and efficient authentication for various applications.

3.2 Malicious user and legitimate user detection performance analysis

MU and LU detection accuracy of our proposed authentication framework is evaluated by the following four detection rates.

(i) Correct detection rate of LU: If the number of iterations is η and the number of detected LUs is β_{LU} then the correct detection rate of LU is defined as follows:

$$R_{LU} = \frac{\beta_{LU}}{\eta} \tag{4}$$

(ii) Correct detection rate of MU: If the number of iterations is η and the number of detected MUs is β_{LU} then the correct detection rate of MU is defined as follows:

$$R_{MU} = \frac{\beta_{MU}}{\eta} \tag{5}$$

(iii) Mis-detection rate of LU: If the number of iterations is η and the number of undetected LUs is $\overline{\beta}_{LU}$ where the LU is present then the mis-detection rate of the LU is defined as follows:

$$\overline{R}_{LU} = \frac{\overline{\beta}_{LU}}{\eta} \tag{6}$$

(iv) Mis-detection rate of MU: If the number of iterations is η and the number of undetected MUs is $\overline{\beta}_{MU}$ where the MU is present then the mis-detection rate of the MU is defined as follows:

$$\overline{R}_{MU} = \frac{\overline{\beta}_{MU}}{\eta} \tag{7}$$

In wireless networking, false positives and false negatives are terms used to describe errors in the detection of threats, such as malicious user, malware, intrusions, or other security breaches. A false positive occurs when a security system incorrectly identifies benign activity as malicious. A false negative occurs when a security system fails to identify actual malicious activity, allowing a threat to go unnoticed.

Effective wireless network security measures aim to balance the rates of false positives and false negatives to ensure optimal protection while minimizing disruptions and resource wastage. This involves fine-tuning detection algorithms, using advanced threat intelligence, and continuously updating security protocols. To minimize the false positives and false negatives in our proposed framework, we have optimized the authentication system design and configuration.

3.3 Spectrum sensing performance analysis

In this subsection, we calculate the probability of detection (P_d) and probability of false alarm (P_f) for our proposed authentication framework based on the MRC fusion rule for two conditions, namely when the CRV is stationary and mobile.

First of all, we measure the energy level of the obtained PU signal at the i^{th} CRV which is found as

$$E_i(MRC) = \sum_{k=0}^{L-1} |y_i(k)|^2 \tag{8}$$

In MRC fusion rule, each CRV multiplies the received energy level ($e_i(MRC)$) with a weight (w_i) and this multiplication result is sent to the corresponding FC. At the FC, all the received test statistical values from the CRVs are added and this additional result is compared with the global threshold λ_{FC} value to take the global decision whether the PU signal is present or absent in the CR-IoV networks. The total energy level ($E^{CSS}(MRC)$) for the MRC fusion rule at the FC is given as follows:

$$E_{CSS}(MRC) = \sum_{i=1}^{N} w_i E_i(MRC) \tag{9}$$

where w_i indicates the weight value and this weight value depends on the SNR (γ) value of the certain CRV [41], which is calculated as follows:

$$w_i = \frac{\gamma_i}{\sqrt{\sum_{i=1}^{N} \gamma_i^2}} \tag{10}$$

When L is large enough, according to the Central Limit Theorem (CLT), E_{CSS} is normally distributed for N CRVs under both H_0 and H_1 hypotheses and we can calculate the Probability Distribution Function (PDF) [42], which is given as follows:

$$E_{CSS} \sim \begin{cases} \left(NL\sigma_n^2, \quad NL\sigma_n^4\right), & : H_0 \\ \left(NL(1+\gamma)\sigma_n^2, \quad NL(1+2\gamma)\sigma_n^4\right), & : H_1 \end{cases} \tag{11}$$

Eq. *(11)* is applicable for any type of modulation technique and noise.

3.3.1 Spectrum sensing evaluation for CRV-stationarity and PU-activity

The FC takes a final global decision about the condition of the received PU signal (i.e., active or idle), which is dependent on the energy level of PU signal E_{CSS}, global threshold λ_c value. The FC calculates the probability of detection, $P_d^{FC}(\lambda_c)$ and probability of false alarm, $P_f^{FC}(\lambda_c)$ as follows [29, 41]:

$$\begin{aligned} P_d^{FC}(\lambda_c) &= Pr[E_{CSS} \geq \lambda_c | H_1] \\ &= Q\left(\frac{\lambda_c - L\sum_{i=1}^{N} w_i(1+\gamma_i)}{\sqrt{2L\sum_{i=1}^{N} w_i(1+2\gamma_i)}}\right) \end{aligned} \tag{12}$$

and

$$P_f^{FC}(\lambda_c) = Pr[E_{CSS} \geq \lambda_c | H_0] = Q\left(\frac{\lambda_c - L\sum_{i=1}^{N} w_i}{\sqrt{2L\sum_{i=1}^{N} w_i^2}}\right) \quad (13)$$

In the proposed authentication framework, the sensing gain ($P_d^{FC}(\lambda_c)$) is improved over the conventional unsecured CSS scheme.

3.3.2 Spectrum detection evaluation for CRV-mobility and PU-activity

The FC makes a global decision on the presence of the PU signal, then the E_{CSS}^{pro} is compared with a corresponding threshold λ_C and velocity of a CRV user. The probabilities of detection, $P_d^{FC}(\lambda_c)$ and false alarm, $P_f^{FC}(\lambda_c)$, are given as follows:

$$P_d^{FC}((\lambda_c), B) = Pr[E_{CSS} \geq \lambda_c | H_1, B] \times Pr[B] = Q\left(\frac{\lambda_c - L\sum_{i=1}^{N} w_i(1+\gamma_i)}{\sqrt{2L\sum_{i=1}^{N} w_i(1+2\gamma_i)}}\right) \times Pr[B] \quad (14)$$

and

$$P_f^{FC}(\lambda_c, A) = Pr[E^{CSS} \geq \lambda_c | H_0, A] \times Pr[A] = Q\left(\frac{\lambda_c - L\sum_{i=1}^{N} w_i}{\sqrt{2L\sum_{i=1}^{N} w_i^2}}\right) \times Pr[A] \quad (15)$$

where $Pr[B]$ denotes the probability for event B when the PU is outside of the CRV's sensing range, which is indicated by event B (i.e., inactive status of PU). When each CRV is dynamic, the $Pr[B]$ can be represented as follows [43]:

$$Pr[B] = \int_0^t \int_0^{\bar{v}} v \frac{1}{\sqrt{2\pi}\sigma_v}\left[exp\left(-\frac{(v-\mu_v)^2}{2\sigma_v^2}\right)\right]^2 dvdt \quad (16)$$

We can calculate the probability for event A when the PU is inside of the CRV's sensing range, which is indicated by event A (i.e., active status of PU). The $Pr[A]$ is given as follows:

$$Pr[A] = 1 - Pr[B] \quad (17)$$

When the velocity of the CRV is modelled according to Gaussian distribution with minimum velocity $v_{min} = \mu_v - 3\sigma_v$ and maximum velocity $v_{max} = \mu_v + 3\sigma_v$, where μ_v indicates an average velocity and σ_v indicates the standard deviation, the probability density function is expressed as follows [43]:

$$\delta_v(v) = \frac{\rho_v(v)}{\int_{v_{min}}^{v_{max}} \rho_v(v)dv} \quad (18)$$

where $\rho_v(v)$ indicates the Gaussian probability density function. The $\rho_v(v)$ can be expressed as:

$$\rho_v(v) = \frac{1}{\sigma_v\sqrt{2\pi}} e^{\left(\frac{-(v-\mu_v)^2}{2\sigma_v^2}\right)} \quad (19)$$

Eq. *(18)* can be updated according to Eq. *(19)* as follows:

$$\delta_v(v) = \frac{2\rho_v(v)}{erf\left(\frac{v_{max}-\mu_v}{\sigma_v\sqrt{2}}\right) - erf\left(\frac{v_{min}-\mu_v}{\sigma_v\sqrt{2}}\right)} \quad (20)$$

where $erf(.)$ is the error function. The expected value of velocity for CRV is expressed as follows:

$$E[V] = \bar{v} = \int_{v_{min}}^{v_{max}} v\delta_v(v)dv \quad (21)$$

Next, the instantaneous velocity $v(t)$ of the CRV at the time t can be represented as follows:

$$v(t) = v = v(0) + \int_0^t a(z)dz \quad (22)$$

where $v(0)$ and $a(z)$ are the initial velocity and the acceleration of the CRV, respectively.

3.4 Global error probability analysis

The global error probability P_e for our proposed digital signature-based secure CSS scheme at the FC can be measured as follows [44]:

$$Pe_{CSS}^{p} = P(H_0)P_f^{FC}(\lambda_c) + P(H_1)\left(1 - P_d^{FC}(\lambda_c)\right) \quad (23)$$

where $P(H_1)$ indicates the probability of activeness and $P(H_0)$ indicates the probability of idleness of the PU in the CR-IoV networks.

3.5 Time delay analysis for making global decisions at the fusion centre

The FC makes a global decision about the presence or absence of the primary user in the CR-IoV networks based on the sensing data of CRVs. Total time delay for making global decisions at the fusion centre depends on the following time factors:

- Spectrum Sensing Time (τ_{SST}): This time is taken by the CRV to detect the presence or absence of the PU in the CR-IoV networks.
- Digital Signature Generation Time (τ_{DSGT}): This time is needed to generate the digital signature at the CRV.
- Reporting Time (τ_{RT}): This time is needed to transmit the encrypted sensing data from the CRV to the FC.
- Digital Signature Verification Time (τ_{SDSVT}): This time is needed to verify the digital signature of the FC.

- Sensing Data Processing Time (τ_{SDPT}): This time is taken by the FC to make the global decision about the presence or absence of the PU in the CR-IoV networks. The FC makes the global decision by applying the fusion rule on the sensing data.

Therefore, the total time required for making global decisions at the fusion centre is calculated by using the following equation:

$$T_d = \tau_{SST} + \tau_{DSGT} + \tau_{RT} + ((N+M) \times \tau_{DSVT}) + \tau_{SDPT} \quad (24)$$

where T_d is the total time required for making the global decision about the presence or absence of the PU in the CR-IoV networks.

3.6 Computational overhead and scalability analysis of the proposed framework

For the CSS scheme without a cluster, the traffic overhead at the FC increases with a growing number of antennas M and CRV users Z. In our proposed framework, the traffic overhead at the FC, considering that during a specific sensing interval each CRV user in the IoV network receives L signal samples with B bits per sample, resulting in the transmission of $L \times B \times M$ bits to the corresponding FC, is given as follows:

$$TO_{FC}^{CSS} = (L \times B \times M \times Z) \quad (25)$$

Scalability in CR-IoV networks refers to the ability of the network to handle an increasing number of CRV users, or traffic without significant performance degradation. Scalability in our CR-IoV networks depends on the number of FCs and processing speed of FC. If we increase the number of FC and processing speed of FC then we can add new CRV users.

4. SIMULATION OUTCOMES AND DISCUSSION

In this section, the experimental outcomes and the associated discussion are exposed. Numerical analyses are conducted and compared with the conventional schemes to evaluate the efficiency of the proposed scheme. The simulation parameters used are listed in Table 1.

Fig. 5 shows the correct detection rate of the LU and the mis-detection rate of theLU for different SNR values for both mobile and stationary CRVs. The results show that our proposed authentication framework can detect the LU with 100% accuracy for different SNR values. The mis-detection rate of the LU is 0% for the proposed authentication framework for different SNR values.

Fig. 6 shows the correct detection rate of an MU and the mis-etection rate of the MU for different SNR values

Table 1 – Parameters used in simulations.

Parameter	Value
The number of legitimate CRVs, N	16
The number of malicious users, M	4
Sampling frequency, f_s	300 kHz
The number of samples, L	2400
Spectrum sensing time of CRV, τ_{SST}	4 ms
Reporting time of CRV, τ_{RT}	2 ms
Digital signature generation time, τ_{DSGT}	31.61 μs
Digital signature verification time, τ_{DSVT}	47.34 μs
Sensing data processing time, τ_{SDPT}	2 ms
Transmitted signal of the PU, $x(l)$	QPSK
The SNR value, γ	[-20 to 0] dB
The vehicle moves with velocity, v	[60, 80] Km/h
The channel noise type, $n(k)$	AWGN

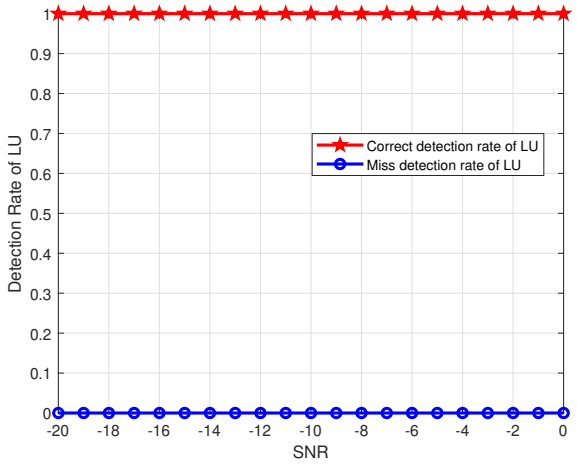

Figure 5 – Correct and mis-etection rate of LU across different values of SNR for mobile and stationary CRVs.

for both mobile and stationary CRVs. The results show that our proposed authentication framework can detect an MU with 100% accuracy for different SNR values. The mis-detection rate of the LU is 0% for the proposed scheme for different SNR values.

From figures 5 and 6, we observed that the detection performance of our proposed spectrum sensing scheme is robust for different SNR values because the detection performance of the digital signature is not dependent on SNR values.

The sensing gain when each CRV is stationary: Fig. 7 shows the probability of detection (P_d) versus probability of false alarm (P_f) curve for the proposed authentication framework and the conventional scheme at the FC. It is observed that our proposed authentication framework achieves better sensing gain (98%) than conventional

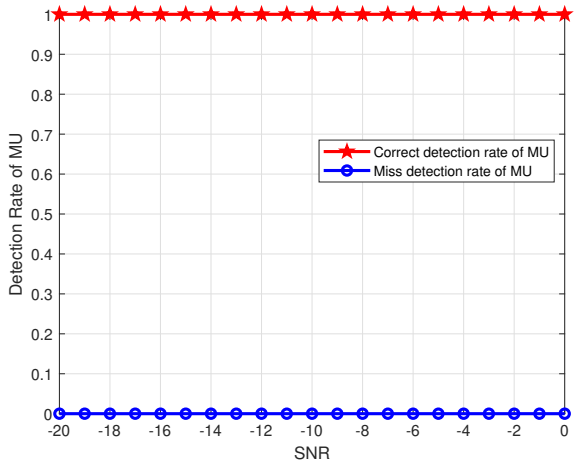

Figure 6 – Correct and mis-detection rate of MU across different values of SNR for mobile and stationary CRVs.

scheme (83%) at the $P_f = 0.1$, when the SNR value is $\gamma = -18$. The proposed authentication framework identifies the MUs and ignores their sensing data, which is why the proposed scheme achieves better sensing gain.

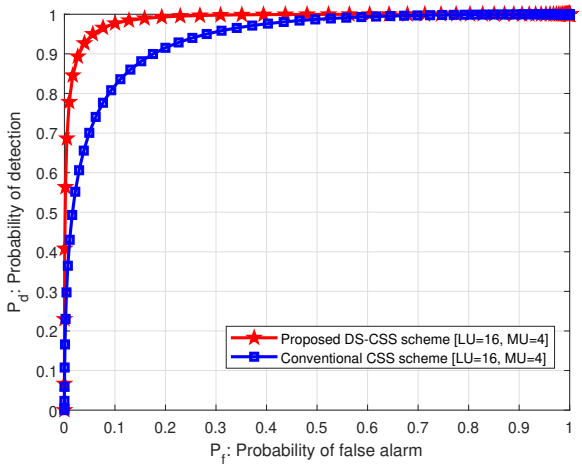

Figure 7 – P_d vs. P_f of the proposed DS-CSS scheme and the conventional scheme for stationary CRV and $\gamma = -18$dB.

The sensing gain when each CRV is mobile: When each CRV is mobile and the PU is stationary in the CR-enabled IoV networks, Fig. 7 shows the P_d versus P_f curve for our proposed authentication framework and the conventional scheme at the FC.

It can be seen that the P_d decreases with the increase in CRV velocity for both the proposed scheme and the conventional scheme. The velocity of the CRV reduces the sensing duration of the CRV to detect the PU signal. That is why the probability of detection has decreased. However, the proposed scheme achieves better sensing gain than the conventional scheme for different velocity of the CRV. From Fig. 8, we can observe that the sensing gain (at $P_f = 0.1$) for the proposed scheme is 90% and 63% when the CRV's velocity is $60Km/h$ and $80Km/h$,

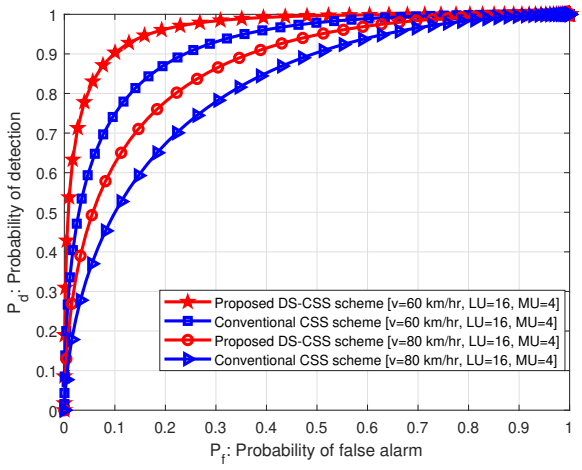

Figure 8 – P_d vs. P_f of the proposed authentication framework and the conventional scheme for mobile CRV, $\gamma = -18$dB and $v = [60, 80]$ Km/h

respectively. Whereas the sensing gain (at $P_f = 0.1$) for the conventional scheme is 75% and 50% when the CRV's velocity is $60Km/h$ and $80Km/h$, respectively.

The global error probability (P_e) when each CRV is stationary: Fig. 9 shows the global error probability (P_e) versus the probability of false alarm (P_f) curve for the proposed scheme and conventional scheme when $LU = 16$ and $MU = 4$. It is observed that the P_e for the proposed scheme is lower than the conventional scheme.

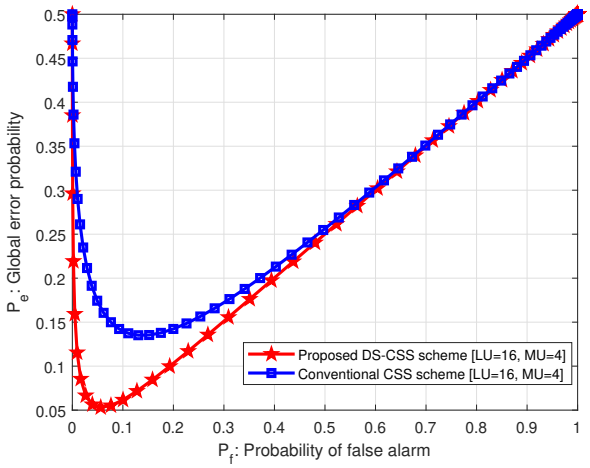

Figure 9 – P_e vs. P_f of the proposed scheme and the conventional scheme for stationary CRV.

The global error probability (P_e) when each CRV is mobile: Fig. 10 shows the P_e versus P_f for the proposed digital signature-based authentication framework and conventional (without security technique) scheme when $LU = 16$, $MU = 4$ and each CRV is mobile in the CR-enabled IoV networks.

From Fig. 10, we can be observe that at the $P_f = 0.1$, the

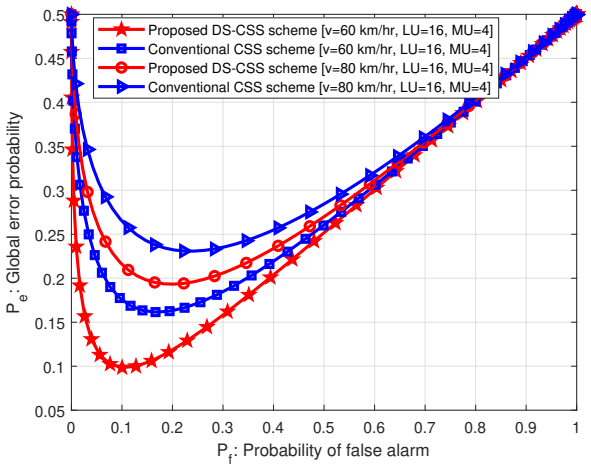

Figure 10 – P_e vs. P_f of the proposed scheme and the conventional scheme for mobile CRV.

P_e of our proposed scheme is 0.1 and 0.21 when the CRV velocity is 60 Km/h and 80 Km/h, respectively; whereas the global error probability for the conventional scheme is 0.18 and 0.27 when the CRV velocity is 60 Km/h and 80 Km/h, respectively. Basically, the P_e value increases slowly with the velocity of the CRV when PU is stationary. From figures 9 and 10, it can be concluded that the proposed digital signature-based secure CSS scheme provides the lowest P_e value relative to the conventional (without security technique) scheme.

4.1 Total time delay for making the global decision at FC:

The total time delay for making the global decision at FC for our proposed approach is calculated by using Eq. *(24)* as follows:

$$\begin{aligned} T_d &= \tau_{SST} + \tau_{DSGT} + \tau_{RT} + ((N+M) \times \tau_{DSVT}) + \tau_{SDPT} \\ &= 4ms + 31.61\mu s + 2ms + (20 \times 47.34\mu s + 2ms \\ &= 8.949ms \end{aligned} \tag{26}$$

4.2 Efficiency analysis

The time (key generation, signature and verification, etc.) and space (data memory, program memory, bandwidth, code and data length, etc.) constraints of the wireless communication network (data memory, program memory, bandwidth, code and data length, etc.) prevent security objectives from being fully achieved. In addition, wireless devices have limited computer power and storage capacity. This necessitates that the digital signature system used in wireless communication networks be as efficient as feasible while upholding security. In this section, we analyze the efficiency of signature generation and signature verification of our proposed framework.

We compare the efficiency of the proposed framework with the Parvin et al. [36], the Manohar et al. [45], the Prashar et al. [46], the Zhang et al. [47], the Tofiq et al. [48], Evelyn et al. [27], and Ashish et. al [28] schemes. The comparison results of signature generation and signature verication are shown in Table 2 and Table 3, respectively. In this table, DPA denotes double-point arithmetic, MM indicates the modular multiplication, and MI indicates the modular inversion.

Table 2 – Comparison of the computational complexity of signature generation

References	DPA	MM	MI
Parvin et al.[36]	2	3	0
Manohar et al.[45]	4	3	1
Prashar et al.[46]	1	2	0
Zhang et al.[47]	1	2	1
Tofiq et al.[48]	1	2	1
Evelyn et al.[27]	1	2	1
Ashish et al.[28]	1	1	1
Proposed scheme	1	1	0

Table 3 – Comparison of the computational complexity of signature verication

References	DPA	MM	MI
Parvin et al.[36]	2	1	1
Manohar et al.[45]	0	3	0
Prashar et al.[46]	1	1	1
Zhang et al.[47]	2	2	1
Tofiq et al.[48]	1	1	0
Evelyn et al.[27]	1	2	1
Ashish et al.[28]	1	2	0
Proposed scheme	1	0	0

Considering that the data scale of one modular multiplication is t, the complexity of one double-point arithmetic is $O(t^2)$, the complexity of one modular multiplication is $O(t^2 \log_2(t))$, and the complexity of one modular inversion is $O(9t^2)$ [49].

Based on Table 2 and Table 3, the total computational complexity of the proposed scheme is $C_1 = O[(\log_2 t + 2)t^2]$, the total computational complexity of the Ashish et al.[28] scheme is $C_2 = O[(3\log_2 t + 11)t^2]$, the total computational complexity of the Evelyn et al.[27] scheme is $C_3 = O[(4\log_2 t + 20)t^2]$, the total computational complexity of the Tofiq et al. [48] scheme is $C_4 = O[(3\log_2 t + 11)t^2]$, the total computational complexity of the Zhang et al. [47] scheme is $C_5 = O[(4\log_2 t + 21)t^2]$, the Prashar et al. [46] $C_6 = O[(3\log_2 t + 11)t^2]$, the total computational complexity of the Manohar et al. [45] scheme is $C_7 = O[(6\log_2 t + 13)t^2]$, the total computational complexity of the Parvin et al. [36] scheme is $C_8 = O[(4\log_2 t + 13)t^2]$. Therefore, the total computational complexity of the proposed framework is much smaller than other exiting schemes.

4.3 among security schemes

Table 4 presents a comparison of our proposed framework with five other security management frameworks in security metrics, which indicate that the proposed framework provides more security than other frameworks, according to security metrics.

Table 4 – Comparison between trust management schemes on security metrics

References	Accuracy	Privacy	Integrity
Parvin et al.[36]	Medium	Low	Low
Manohar et al.[45]	Medium	Medium	Low
Prashar et al.[46]	Medium	Low	Medium
Zhang et al.[47]	High	Medium	Low
Tofiq et al.[48]	Medium	Medium	High
Evelyn et al.[27]	Medium	Medium	High
Ashish et al.[28]	High	Medium	High
Proposed scheme	High	High	High

5. CONCLUSIONS AND FUTURE WORK

In this article, we evaluated the performance of the proposed digital signature-based authentication framework. In the LU and MU detection accuracy rate, the proposed digital signature-based authentication framework provides 100% correct detection and 0% mis-detection rate for both LU and MU. However, the detection process increases the processing time due to the additional communication overhead. In the sensing gain, the proposed digital signature based secure CSS scheme achieves 15% better spectrum sensing gain than the conventional scheme for both conditions, either when the CRV is stationary or mobile.

The global error probability of the proposed digital signature-based secure CSS scheme is 8% lower than the conventional scheme for both conditions, either when CRV is stationary and mobile. The total time delay for making the global decision at FC for our proposed scheme is 8.949ms. Therefore, we conclude that our proposed digital signature-based authentication framework will be more suitable for CR-IoV networks due to the fact that it minimizes the issue of spectrum deficit, prevents the malicious user attack, enhances the sensing gain and achieves lower global error probability than the conventional (without security technique) scheme.

In the future, we plan to increase the security and efficiency of the proposed authentication framework in the context of CR technology and IoV networks with several key areas of focus: machine learning for anomaly detection machine-learning algorithms can be integrated to detect anomalies in real-time, ensuring that any unusual behaviour is promptly identified and addressed. This could involve using supervised learning for known threats and unsupervised learning for unknown threats. Blockchain for decentralized key management-Blockchain technology can provide a decentralized and tamper-proof system for managing authentication keys, ensuring that no single point of failure exists.

ACKNOWLEDGEMENT

This research was supported in part by the Department of Information and Communication Engineering, and the Research Cell of Noakhali Science and Technology University (NSTU), Noakhali, 3814, Bangladesh, in part by project IRENE-EARTH (PID2020-115323RBC33/AEI/10 .13 039/501100011033), and in part by Bangladesh Bureau of Educational Information & Statistics (BANBEIS), Ministry of Education, Government of the Peoples Republic of Bangladesh (IC20201325).

REFERENCES

[1] Marwa Mamdouh, Mohamed AI Elrukhsi, and Ahmed Khattab. "Securing the internet of things and wireless sensor networks via machine learning: A survey". In: *2018 International Conference on Computer and Applications (ICCA)*. IEEE. 2018, pp. 215–218.

[2] Mohammad Nuruzzaman Bhuiyan, Md Masum Billah, Farzana Bhui, Md Ashikur Rahman Bhuiyan, Nazmul Hasan, Md Mahbubur Rahman, Md Sipon Miah, Farhad Alibakhshikenari Mohammad, Francisco Falcone, et al. "Design and Implementation of a Feasible Model for the IoT Based Ubiquitous Healthcare Monitoring System for Rural and Urban Areas". In: *IEEE Access* 10 (2022), pp. 91984–91997.

[3] Md Sipon Miah and Insoo Koo. "An Automatic Road Sign Recognizer for an Intelligent Transport System". In: *Journal of information and communication convergence engineering* 10.4 (2012), pp. 378–383.

[4] Yangxin Lin, Ping Wang, and Meng Ma. "Intelligent transportation system (its): Concept, challenge and opportunity". In: *2017 ieee 3rd international conference on big data security on cloud (bigdatasecurity), ieee international conference on high performance and smart computing (hpsc), and ieee international conference on intelligent data and security (ids)*. IEEE. 2017, pp. 167–172.

[5] Keyvan Ansari. "Joint use of DSRC and C-V2X for V2X communications in the 5.9 GHz ITS band". In: *IET Intelligent Transport Systems* 15.2 (2021), pp. 213–224.

[6] Gautami Tripathi, Mohd Abdul Ahad, and Mithileysh Sathiyanarayanan. "The Role of Blockchain in Internet of Vehicles (IoV): Issues, Challenges

and Opportunities". In: *2019 International Conference on contemporary Computing and Informatics (IC3I)*. IEEE. 2019, pp. 26–31.

[7] Faroq A Awin, Yasser M Alginahi, Esam Abdel-Raheem, and Kemal Tepe. "Technical issues on cognitive radio-based Internet of Things systems: A survey". In: *IEEE Access* 7 (2019), pp. 97887–97908.

[8] Rajith C Abeywardana, Kevin W Sowerby, and Stevan M Berber. "Empowering Infotainment Applications: A Multi-Channel Service Management Framework for Cognitive Radio Enabled Vehicular Ad Hoc Networks". In: *2018 IEEE 87th Vehicular Technology Conference (VTC Spring)*. IEEE. 2018, pp. 1–5.

[9] Lin Cheng, Benjamin E Henty, Daniel D Stancil, Fan Bai, and Priyantha Mudalige. "Mobile vehicle-to-vehicle narrow-band channel measurement and characterization of the 5.9 GHz dedicated short range communication (DSRC) frequency band". In: *IEEE Journal on Selected Areas in Communications* 25.8 (2007), pp. 1501–1516.

[10] Mohammad Amzad Hossain, Michael Schukat, and Enda Barrett. "Enhancing the Spectrum Sensing Performance of Cluster-Based Cooperative Cognitive Radio Networks via Sequential Multiple Reporting Channels". In: *Wireless Personal Communications* (2020), pp. 1–23.

[11] Wei Yao, Abid Yahya, Fazlullah Khan, Zhiyuan Tan, Ateeq Ur Rehman, Joseph M Chuma, Mian Ahmad Jan, and Muhammad Babar. "A secured and efficient communication scheme for decentralized cognitive radio-based Internet of vehicles". In: *IEEE Access* 7 (2019), pp. 160889–160900.

[12] Joy Eze, Sijing Zhang, Enjie Liu, and Elias Eze. "Cognitive radio-enabled internet of vehicles: a cooperative spectrum sensing and allocation for vehicular communication". In: *IET Networks* 7.4 (2018), pp. 190–199.

[13] Hussein Kobeissi, Youssef Nasser, Amor Nafkha, Oussama Bazzi, and Yves Louet. "On the detection probability of the standard condition number detector in finite-dimensional cognitive radio context". In: *EURASIP Journal on Wireless Communications and Networking* 2016.1 (2016), pp. 1–11.

[14] Mengwei Sun, Chenglin Zhao, Su Yan, and Bin Li. "A novel spectrum sensing for cognitive radio networks with noise uncertainty". In: *IEEE Transactions on Vehicular Technology* 66.5 (2016), pp. 4424–4429.

[15] Ankit Singh Rawat, Priyank Anand, Hao Chen, and Pramod K Varshney. "Collaborative spectrum sensing in the presence of Byzantine attacks in cognitive radio networks". In: *IEEE Transactions on Signal Processing* 59.2 (2010), pp. 774–786.

[16] Rüstem YILMAZEL and Muhammet Nuri SEYMAN. "Cooperative spectrum sensing method for MC-CDMA systems in cognitive radio networks". In: *2018 6th International Conference on Control Engineering & Information Technology (CEIT)*. IEEE. 2018, pp. 1–5.

[17] Adnan Sajid, Bilal Khalid, Mudassar Ali, Shahid Mumtaz, Usman Masud, and Farhan Qamar. "Securing cognitive radio networks using blockchains". In: *Future Generation Computer Systems* 108 (2020), pp. 816–826.

[18] Abitha Kumari Duraisamy, Raja Guru Ramaraj, Mathankumar Manoharan, and Manjunathan Alagarsamy. "Certificateless linkable ring signature-based blockchains for securing cognitive radio networks". In: *Concurrency and Computation: Practice and Experience* 34.24 (2022), e7235.

[19] Anand Paul, Alfred Daniel, Awais Ahmad, and Seungmin Rho. "Cooperative cognitive intelligence for internet of vehicles". In: *IEEE Systems Journal* 11.3 (2015), pp. 1249–1258.

[20] Muhammad Sajjad Khan, Muhammad Jibran, Insoo Koo, Su Min Kim, and Junsu Kim. "A double adaptive approach to tackle malicious users in cognitive radio networks". In: *Wireless Communications and Mobile Computing* 2019 (2019).

[21] Md Sipon Miah, Md Shamim Hossain, and Ana Garcia Armada. "Machine Learning-based Malicious Users Detection in Blockchain-Enabled CR-IoT Network for Secured Spectrum Access". In: *2022 IEEE International Symposium on Broadband Multimedia Systems and Broadcasting (BMSB)*. IEEE. 2022, pp. 1–6.

[22] Mohammed Abdulhakim Al-Absi, Ahmed Abdulhakim Al-Absi, and Hoon Jae Lee. "A secure enhanced non-cooperative cognitive division multiple access for vehicle-to-vehicle communication". In: *Sensors* 20.4 (2020), p. 1000.

[23] Jie Cui, Jing Zhang, Hong Zhong, and Yan Xu. "SPACF: A secure privacy-preserving authentication scheme for VANET with cuckoo filter". In: *IEEE transactions on vehicular technology* 66.11 (2017), pp. 10283–10295.

[24] Neelam Dewangan and RN Kumar. "A framework for secure cooperative spectrum sensing based with blockchain and deep learning model in cognitive radio". In: *2023 International Conference on Artificial Intelligence and Knowledge Discovery in Concurrent Engineering (ICECONF)*. IEEE. 2023, pp. 1–6.

[25] Sachin Sharma and Seshadri Mohan. "Cognitive radio adhoc vehicular network (CRAVENET): Architecture, applications, security requirements and challenges". In: *2016 IEEE international conference on advanced networks and telecommunications systems (ANTS)*. IEEE. 2016, pp. 1–6.

[26] Sazia Parvin, Farookh Khadeer Hussain, and Omar Khadeer Hussain. "Digital signature-based authentication framework in cognitive radio networks". In: *Proceedings of the 10th International Conference on Advances in Mobile Computing & Multimedia*. 2012, pp. 136–142.

[27] Evelyn Ezhilarasi, J Christopher Clement, et al. "Robust Cooperative spectrum sensing in Cognitive Radio Blockchain network using SHA-3 algorithm". In: *Blockchain: Research and Applications* (2024), p. 100224.

[28] Ashish Khanna, Tariq Hussain Rani Poonam, Vineet Gupta, and Joel JPC Rodrigues. "Blockchain-based security enhancement and spectrum sensing in cognitive radio network". In: *Wireless Personal Communications* 127.3 (2024), pp. 1899–1921.

[29] Md Sipon Miah, Michael Schukat, and Enda Barrett. "Maximization of sum rate in AF-cognitive radio networks using superposition approach and n-out-of-k rule". In: *2017 28th Irish signals and systems conference (ISSC)*. IEEE. 2017, pp. 1–6.

[30] Wang Weifang. "Denial of service attacks in cognitive radio networks". In: *2010 The 2nd Conference on Environmental Science and Information Application Technology*. Vol. 2. IEEE. 2010, pp. 530–533.

[31] N Gayathri, H Anandakumar, S Gowri, J Keerthika, and S Nithyapriya. "An analysis of Network Security Attacks and their mitigation for Cognitive Radio Communication". In: *2023 9th International Conference on Advanced Computing and Communication Systems (ICACCS)*. Vol. 1. IEEE. 2023, pp. 2413–2417.

[32] Mampuele Lebepe and Mthulisi Velempini. "Mitigation of Denial of Service Attacks in Software-Defined Cognitive Radio Networks". In: *2021 International Conference on Artificial Intelligence, Big Data, Computing and Data Communication Systems (icABCD)*. IEEE. 2021, pp. 1–5.

[33] Ishu Gupta and OP Sahu. "An Overview of primary user emulation attack in cognitive radio networks". In: *2018 Second International Conference on Computing Methodologies and Communication (ICCMC)*. IEEE. 2018, pp. 27–31.

[34] Xin Liu, Can Sun, Mu Zhou, Bin Lin, and Yuto Lim. "Reinforcement learning based dynamic spectrum access in cognitive internet of vehicles". In: *China Communications* 18.7 (2021), pp. 58–68.

[35] Mohammad Amzad Hossain, Michael Schukat, and Enda Barrett. "Enhancing the Spectrum Utilization in Cellular Mobile Networks by Using Cognitive Radio Technology". In: *2019 30th Irish Signals and Systems Conference (ISSC)*. IEEE. 2019, pp. 1–6.

[36] Sazia Parvin and Farookh Khadeer Hussain. "Digital signature-based secure communication in cognitive radio networks". In: *2011 International Conference on Broadband and Wireless Computing, Communication and Applications*. IEEE. 2011, pp. 230–235.

[37] Arif Mughal, Xiong Luo, Ata Ullah, Subhan Ullah, and Zahid Mahmood. "A lightweight digital signature based security scheme for human-centered Internet of Things". In: *IEEE Access* 6 (2018), pp. 31630–31643.

[38] Mohamad Ali Sadikin and Septia Ulfa Sunaringty. "Implementing digital signature for the secure electronic prescription using QR-code based on android smartphone". In: *2016 International Seminar on Application for Technology of Information and Communication (ISemantic)*. IEEE. 2016, pp. 306–311.

[39] Zibin Zheng, Shaoan Xie, Dai, and Xiangping Chen. "An overview of blockchain technology: Architecture, consensus, and future trends". In: *2017 IEEE international congress on big data (BigData congress)*. IEEE. 2017, pp. 557–564.

[40] Farah Jihan Aufa, Achmad Affandi, et al. "Security system analysis in combination method: RSA encryption and digital signature algorithm". In: *2018 4th International Conference on Science and Technology (ICST)*. IEEE. 2018, pp. 1–5.

[41] Sumi and RS Ganesh. "Improved EGC method for increasing detection in cognitive radio network". In: *Computer Communications* 147 (2019), pp. 127–137.

[42] Md Sipon Miah, Michael Schukat, and Enda Barrett. "An enhanced sum rate in the cluster based cognitive radio relay network using the sequential approach for the future Internet of Things". In: *Human-centric Computing and Information Sciences* 8.1 (2018), pp. 1–27.

[43] Danda B Rawat, Reham Alsabet, Chandra Bajrach, and Min Song. "On the performance of cognitive internet-of-vehicles with unlicensed user-mobility and licensed user-activity". In: *Computer Networks* 137 (2018), pp. 98–106.

[44] Md Sipon Miah, Michael Schukat, and Enda Barrett. "Sensing and throughput analysis of a MU-MIMO based cognitive radio scheme for the Internet of Things". In: *Computer Communications* 154 (2020), pp. 442–454.

[45] Anita Latsmi Manohar, Kok-Lim Alvin Yau, Mee Hong Ling, and Suleman Khan. "A security enhanced cluster size adjustment scheme for cognitive radio networks". In: *IEEE Access* 7 (2018), pp. 117–130.

[46] Deepak Prashar, Mamoon Rashid, Shams Tabrez Siddiqui, Dilip Kumar, Amandeep Nagpal, Ahmed Saeed AlGhamdi, and Sultan S Alshamrani. "SDS-WSNa secure approach for a hop-based localization algorithm using a digital signature in the wireless sensor network". In: *Electronics* 10.24 (2021), p. 3074.

[47] Ping Zhang, Yamin Li, Muhua Liu, Youlin Shang, and Zhumu Fu. "An ECC-Based Digital Signature Scheme for Privacy Protection in Wireless Communication Network". In: *Wireless Communications and Mobile Computing* 2022.1 (2022), p. 1977798.

[48] Azzam Khalid Hama Tofiq, Mohammad Fathi, and Faraedoon Waly Ahmed. "A lightweight secure throughput optimization scheme in cognitive radio networks". In: *Wireless Personal Communications* 132.1 (2023), pp. 245–259.

[49] Ai Wan Fan and Shu Xi Lu. "An improved elliptic curve digital signature algorithm". In: *Applied Mechanics and Materials* 34 (2010), pp. 1024–1027.

AUTHORS

Mohammad Amzad Hossain was born in Rajbari, Bangladesh. He received his B.Sc., and M.Sc. from Information and Communication Technology (ICT), at the Islamic University (IU), Kushtia, Bangladesh, in 2010 and 2011, respectively. He received his structured Ph.D. in computer science from University of Galway, Galway, Ireland, in June 2022. He is currently an associate professor in the Department of Information and Communication Engineering, Noakhali Science and Technology University, Noakhali, Bangladesh. His research interests include spectrum sensing, MIMO based cognitive radio networks and cognitive radio based Internet of Things (CR-IoT) networks, machine/deep learning based wireless network, cybersecurity, block-chain based wireless network security. The above research lines have produced more than 17 publications in international journals and presentations within international conferences with a total number of citations of more than 473 and H-index of 7 reported by Google Scholar. He also acts as a referee in several highly reputed journals and international conferences.

Md. Sipon Miah was born in Gaibandha, Bangladesh, in January 1982. He received his B.Sc., M.Sc., and Ph.D. from the Department of Information and Communication Technology (ICT), at the Islamic University, Kushtia-7003, Bangladesh, in 2006, 2007 and 2016, respectively. He received his structured Ph.D. in computer science from University of Galway, Galway, Ireland, in June 2021. Since 2010, he has been with the Department of Information and Communication Technology, in the Islamic University, Kushtia-7003, Bangladesh. He is currently a professor in the Department of ICT, Islamic University, Kushtia-7003, Bangladesh. He is also a postdoctoral fellow in the department of Signal Theory and Communications, University Carlos III of Madrid (UC3M), Leganes, Madrid, Spain. He was a recipient of the three years research grant funded by University Carlos III of Madrid (UC3M) under the prestigious 30 postdoctoral fellowship, started in October 2021, and the four years structured Ph.D. Hardiman Scholarship funded by the University of Galway, Galway, Ireland, started in September 2016. He received the "Teaching Excellent Acknowledgment" Certificate for the course of Simulation and Optimization of Communication Systems from the Vice-Rector of studies of UC3M. He was a visiting professor (short-term) in the department of Energy and Electrical Engineering, Chang'an University, Xian, China. His research interests include cognitive radio-based Internet of things, machine learning/deep learning-based wireless communications, THz communications, optimization-based wireless communications and massive MIMO antennas-based wireless communications. The above research lines have produced more than 70 publications in international journals, presentations within international conferences, and book chapters with a total number of citations of more than 1163 and a H-index of 14 reported by Google Scholar. He is serving as an editorial board member for scientific reports. He also acts as a referee in several highly reputed journals and international conferences.

Ana Garcia Armada received a Ph.D. degree in electrical engineering from the Polytechnic University of Madrid in February 1998. She is currently a professor at Universidad Carlos III de Madrid, Spain. She is leading the Communications Research Group at this university. She has participated in more than 30 national and 10 international research projects, as well as having 20 contracts with the industry. Her research has resulted in nine book chapters, and more than 150 publications in prestigious international journals and conferences, as well as five patents. She has also contributed to standardization organizations (ITU, ETSI) and is a member of the European 5GPPP Group of Experts, as well as the Spanish representative on the committee of the ESA Joint Board on Communication Satellite Programs 5G Advisory Committee (5JAC). She has been editor (20162019, Exemplary Editor Award 2017 and 2018) and area editor (20192020, Exemplary Editor Award 2020) of IEEE Communication Letters.

She has been the editor of IEEE Transactions on Communications since 2019, area editor of IEEE Open Journal of the Communications Society since 2019, editor of the ITU Journal on Future and Evolving Technologies and is a regular member of the technical program committees of the most relevant international conferences in their field. She has formed / is part of the organizing committee of the IEEE Globecom 2019 and 2021 (General Chair), IEEE Vehicular Technology Conference Spring 2018, 2019 and Fall 2018, IEEE 5G Summit 2017, among others. She is Secretary of the IEEE ComSoc Signal Processing and Computing for Communications Committee, has been secretary and chair of the IEEE ComSoc Women in Communications Engineering Standing Committee. Since January 2020 she is Director of Online Content of the IEEE Communications Society. She has received the Award of Excellence from the Social Council and the Award for Best Teaching Practices from Universidad Carlos II de Madrid, as well as the third place Bell Labs Prize 2014, the Outstanding Service Award 2019 from the SPCE committee of the IEEE Communications Society and the Outstanding Service Award 2020 from the Women in Communications Engineering (WICE) standing committee.