Computer Systems Science & Engineering
DOI:10.32604/csse.2022.021543
Article

Tech Science Press

An Effective Secure MAC Protocol for Cognitive Radio Networks

Bayan Al-Amri[1], Gofran Sami[2] and Wajdi Alhakami[1,*]

[1]Department of Information Technology, College of Computers and Information Technology, Taif University, Taif, 21944, Saudi Arabia
[2]Department of Computer Science, Joint First Year Deanship, Umm Al-Qura University, Makkah, 21955, Saudi Arabia
*Corresponding Author: Wajdi Alhakami. Email: whakami@tu.edu.sa
Received: 06 July 2021; Accepted: 07 August 2021

Abstract: The vast revolution in networking is increasing rapidly along with technology advancements, which requires more effort from all cyberspace professionals to cope with the challenges that come with advanced technology privileges and services. Hence, Cognitive Radio Network is one of the promising approaches that permit a dynamic type of smart network for improving the utilization of idle spectrum portions of wireless communications. However, it is vulnerable to security threats and attacks and demands security mechanisms to preserve and protect the cognitive radio networks for ensuring a secure communication environment. This paper presents an effective secure MAC protocol for cognitive radio networks, significantly enhancing the security level of the existing DSMCRN and SSMCRN protocols by eliminating the authentication server's necessity, which can be a single point of failure to compromise the entire network communication. The proposed protocol has proven to be effective and reliable since it does not rely on a centralized entity for providing the required security for a single pair of cognitive users. The protocol also improves the performance in the context of fast switching to data channels leading to higher throughput is achieved compared to the benchmark protocols.

Keywords: Cognitive radio networks; shared key; authentication; elliptic curve cryptography; throughput

1 Introduction

Cognitive Radio (CR) [1] is an expedient technology that overcomes the shortage of spectrum usage in the current wireless networks [2–4]. CR technology rectifies this problem by making good use of the idle spectrum portions (white space), by managing and assigning licensed free channels to Cognitive Users (CUs) (namely Secondary Users) in a legal and organized manner [5]. An outcome of a good utility of an idle spectrum by CUs is what Cognitive Radio Networks (CRNs) offers along with the dynamic features provided increase the numbers of CUs while using the various radio resources in this technology [6–9].

Furthermore, in contrast with the current wireless networking, CRN presents a novel, efficient methods and concepts that provide an effectual procedure based on a dynamic utilization of the spectrum. In comparison, the current wireless domain is set on the assigned radio spectrum along with the licensed

Primary Users (PUs) only and their channels [10]. The main pioneering features of the CRNs are making it an innovative technology, features such as its ability to be cognitive and sorting to the spectrum, which presents active and practical access to the idle portions of the spectrum equally among PUs and CUs upon some features: adapting to the environment, capability to learn for example to evacuate the channel whenever the PU appears, observation, the ability to communicate in any technology environment, awareness regarding the white space areas, and modification inspection [6,11–13]. These features offer a consistent connection between CUs in a practical way regarding the users' time of access and location.

CRN has much smarter utilities and functionalities that are used in the various procedures of the communication, such as Spectrum Sensing, Spectrum Sharing, Spectrum Management, and Spectrum Mobility [6,14,15]. Hence the CRN is distinguished from the current wireless networks because of its complex characteristics mentioned which is why CR domain is recognized as Dynamic Spectrum Access (DSA), and Dynamic Spectrum Management (DSM) [6,8,16].

However, the diverse functionalities of the CRNs are prone to more threats and attacks compared to the traditional wireless networks. Moreover, the demand for security to be implemented in CRNs is for ensuring secure communications; hence some attacks are targeting CR main functionalities of the spectrum, such as the Denial Of Service attacks (DOS), Jamming attacks, and the Primary User Interference (PUI) in the Spectrum sensing phase [6,16,17]. The forgery attack in which the hacker causes Spectrum Management to make false decisions when a false spectrum sensing information is sent to the CUs [14], and in Spectrum Mobility, an issue of a failed hand-off occurs when an attacker would pretend to be a PU to force the CU to evacuate the channel [6,17–19]. Packet forgery that causes DoS in the Spectrum Sharing operation is one of the security threats that are addressed in the security domain of CR networks [6,16,17]. There might also be new types of attacks targeting the CRNs in which this technology is new and is susceptible to such unknown novel threats. In addition, providing defense against many CR threats and attacks represent a serious challenge due to the smart malicious tactics, in contrast with the traditional wireless networks where attacks are more predictable [6,17–20] , preserving security requirements falling under the principles of authentication, integrity, and confidentiality helps to optimize the efficiency of spectrum utilization for secure communications in CRNs.

The paper is organized into 7 sections. Section 2 presents the main contributions of this work, then Section 3 introduces the recent approaches conducted by other researchers to secure the CRN environment, while Section 4 presents the methodology of the proposed protocol and its framework. The implementation and evaluation of the proposed Effective Secure MAC protocol are provided in Section 5. The Comparison of the proposed secure MAC with benchmarks protocols is presented in Section 6. The paper is concluded in Section 7.

2 Contributions

The main contributions achieved in the current work are summarized as follow:

- Eliminating the need for the centralized authentication server in the control phase in DSMCRN and SSMCRN protocols.

The proposed protocol decreases the number of security control frames exchanged between CUs and the authentication server to validate the cognitive users and provide the required security session key for a pair of CUs to secure their communication. Therefore, the successful attempt of eliminating the dedicated server and replacing it with the use of the ECC algorithm, since the dedicated server, can be a single point of failure in case any malicious activity occurs, leading the entire network to be compromised, thus affecting the communication between CUs in the network.

- Reliability and efficiency of the proposed protocol.

The proposed protocol provides a reliable and efficient cognitive radio environment upon the use of the ECC algorithm. This aims to maintain the overall network and make it robust in the presence of any threat targeting the dedicated authentication server. The registered CUs can communicate and establish the required session key using the ECC algorithm, which is known only between the pair of CUs in a single communication, and the generated session key is going to be used to secure their communication including Free Channel List (FCL), Selected Licensed Data Channels (SLDCH), and data exchange without involving the need of the server as it is required in both Digital Signature-based Secure MAC Protocol for CRNs (DSMCRN) and Shared-Key Based Secure MAC Protocol for CRNs (SSMCRN) protocols.

- Improving the performance of the communication time and throughput.

The performance of the proposed protocol has proven to be quite significant compared to the DSMCRN protocol. This is because of less communication time taken over the control channel to exchange the FCL and SLDCH, leading to fast switching to the data channel to initiate the data exchange.

- Higher security level

A higher security level is accomplished because of the greater size of the security session key generated by the ECC algorithm in the proposed protocol. This results in more security compared to the existing shared key produced by the authentication server to a pair of CUs in DSMCRN and SSMCRN protocols.

3 Literature Review

Due to the new nature and characteristics of the CRNs compared to the traditional wireless networks, CRNs are more susceptible to threats and attacks such as Jamming and selfish attacks [6]. Hence the security is still to be more investigated and developed in the CRNs field. Security requirements such as authentication and secure communications between CUs have received big attention in the literature. Consequently, many research works were conducted in the CRNs area to satisfy the security requirements. Therefore, this section focuses on two main authenticating procedure approaches in CRNs: digital signature and shared Key. The dynamic features of the CRN that offer many benefits make it under the threat of lots of dangerous circumstances; this fact has drawn many researchers to conduct more work on the field of security in CRNs [21].

3.1 Digital Signature Cryptography Techniques

Many research contributions in the CR authentication area was conducted with the digital signature techniques, such as in [22] work, when they proposed a security protocol called MSC-MAC, built upon the NTRU's digital signature authentication technique [22], their proposed technique's target was to add more security on the process of changing channels in the CRN, stating that even with a DoS attack is ongoing in the communication, their proposed scheme would help the users switch to another channel in a short time without being affected by the attack, the next safe channel is chosen from the Random out of order List of the Shared Channels (RLSC), the authentication is implemented in the first phase of the connection in the form of a dual authentication, results show that the impact of a DoS is nearly unnoticeable. The security strength of their RLSC and MSC-MAC technique presents a safe shifting operation of channels, and they claim success of resistance against DoS [22]. However, they described this processes as a "quick" switching process [22], yet the digital signature is known to slow up the operation.

According to the authors in the research [23], the need to improve security and maintain a safe and practical networking environment motivated them to present an authentication method and an innovated digital signature model to the CRNs. Their model of the Advanced Digital-Signature-Scheme (DSS) is an improved digital signature model built based on the digital signature and authentication techniques

applied in CRNs; one of its characteristics is that it is an algorithm without a key to simplify it and make it consume less time in the CR networks communication, this algorithm which is built by using a novel adapted hash-function and authentication technique, was examined in equivalence to the existing hash function scheme. Authors assimilated their method with the RSA-DSS, the validity phase was conducted with the OMNeT++. The results showed that the proposed scheme is faster than the current hash function algorithm and has an improved avalanche-effect which indicates whether or not the hashed value has been under any modification, low possibilities of collisions. When integrated with the technique of asymmetric cryptography, results showed a better performance and operational phases. In conclusion, their work preserves authentication, integrity, and the other fundamental security necessities [23].

An authentication protocol based on digital signature was proposed in [24], named DSMCRN. The authentication procedure by the signature is deployed during the registration phase of the connection in the CRN when a public/private keys pair is generated from the to-be registered CU to the server to provide a special ID appended to the received public key from the CU. Then the secure exchanging of data is performed by employing the AES encryption in the data exchange phase. Authentication, confidentiality, and authorization requirements are fulfilled by this approach [25]. However, the use of digital signatures is known to slow up the performance. Hence the duration is a bit long to be considered practical for the CRN's dynamic and fast configurations. Also, the number of exchanged frames can be reduced in which dependence on the server may be dispensed within a couple of frames in the connection.

In [26] research, authors addressed the security and location privacy issues in the cooperative centralized spectrum sensing process. In contrast, the privacy of the CUs IDs can be affected during the interactions between the fusion center and the CUs by a malicious CU, resulting in the association of the IDs with the location of the CUs. Their scheme's concept is about using pseudo IDs rather than the original IDs when interacting with the fusion center to preserve location privacy. Secondly, the authentication process is based upon the elliptic curve cryptography, where it takes place in the sensing phase operation for the fusion center to authenticate sensing requests. Results showed success in decreasing the operation's overhead and better performance in the communication and storage cost along with success in security and location preservation in the proposed scheme [26].

3.2 Shared Key Cryptography Techniques

Another area of research focused on the concept of the shared key technique to preserve authentication rather than using digital signature, like in [27] when the communication in the CRNs is conducted in two main phases of authentication, starting with an initial stage of authentication between the CR node and CR user prior accessing to the CRNs services. A third trusted party is authenticating the CU before allowing access to the network; validation operation includes the use of both the symmetric and public key algorithms, encryption takes place in between CUs in the connection to preserve accessibility and availability, the results are enhanced security, fewer possibilities to be under DOS, reflection, the man in the middle attacks [27]. Note that their model takes place in all layers to authenticate CR nodes, including the network layer, and they claim that applying this one technique on all layers respectively, in the same manner, presents greater security [27]. However, the authentication process may differ in each layer based on its characteristics and how they understand and process information. Their technique takes place in a centralized framework type where the two stations are responsible for the authentication exist, yet this is not quite relevant to *Ad Hoc* CRNs.

A secure MAC protocol known as SMCRN was presented in the CRNs in [28]. The authentication was mainly based on shared key's use generated by the third trusted party to each CU. The aim was to create a secure authentication and communication protocol among CUs that serves the efficiency of less duration time and adds more security in the protocols of the MAC layer of the CR. The protocol is based on the concept of shared key cryptography innovatively. The protocol basically works on three stages: registration, control,

data transmission. Only the first two stages have several frames exchanged between (sender, receiver, and server). The process involves the implementation of a group of shared keys and MAC-Key algorithms. Thus, a session key is generated and delivered by the authentication server to a pair of CUs for securing both the control and data exchange information. The authors analyzed the presented SMCRN protocol by using the Burrows Abadi Needham (BAN) logic method to confirm the security of their protocol from a cryptographic perspective. These analyses performed on all the three stages of the security implementation of the SMCRN protocol, the analysis of security showed success in all three stages. Moreover, the authors evaluated their protocol in terms of the time consumption of the frames for all three stages. They discussed the results by pointing out the advantages of SMCRN in terms of energy efficiency and time of ciphered operations. Results showed that compared to the asymmetric key mechanism, the SMCRN protocol has a faster connection, leading to the advantages of less occupation of the Common Control Channel (CCC), plus the fast switching to the Selected Data Channel List (SDCH), the SMCRN protocol proved effectiveness in the field of CRNs [28]. This protocol preserves authentication, integrity and has a good performance regarding communication time and throughput. However, the achieved performance can be improved by eliminating the use of the authentication server which might lead decreasing the number of exchanged security frames, with consideration of the desired security level.

Another CRNs secure MAC protocol is based on shared key cryptography presented in [25]. So when three different shared keys are generated throughout the communication. The protocol, namely SSMCRN, uses three different shared keys generated throughout the communication to satisfy the security requirements such as confidentiality, authentication, and integrity for CUs. The protocol preserves strong security in between the exchanged frames throughout the CR connection. However, the protocol relies on the presence of the authentication server to process the generation of the shared key that is delivered to a pair of CUs. Thus, the secure exchanging of data is performed by employing the AES encryption in the data exchange phase, ensuring the confidentiality requirement. Results showed better performance in terms of both communication time and throughput than the other benchmarks [25].

Tab. 1 presents and summarizes the overmentioned security approaches conducted by other researchers to secure the CRNs environments successfully.

Table 1: The recent security approaches conducted to secure the cognitive radio networks environment

Ref	Year	Aim	Approach
[22]	2019	Strengthen security during channel switching	A security protocol called MSC-MAC, built based on digital signature, switching process to a channel from RLSC
[23]	2017	Improve security and maintain a safe and practical networking environment	An improved model of the advanced digital-signature-scheme (DSS), this algorithm is built by using a novel adapted hash-function and authentication technique
[24]	2016	Present an authentication protocol on the MAC layer of CRNs based on digital signature technique. Moreover, A MAC layer in CR (MCRN) based secure protocol is presented and it is based on the concept of the shared key cryptography	Authentication procedure conducted by the digital signature is deployed during the registration phase of the connection in the CRN. In addition, the authentication was mainly based on the use of shared key that is generated by the third trusted party to each CU, through three sequential stages.

(Continued)

Table 1 (continued)

Ref	Year	Aim	Approach
[26]	2020	Secure CRN by authenticating CUs from malicious users	All CUs and PUs are represented in the scheme as blocks in the same way as in blockchain, and by the employment of a digital signature technique to validate and authenticate CUs from malicious users.
[27]	2020	Address the security and location privacy issues in the cooperative centralized spectrum sensing process	Using a pseudo IDs rather than the original IDs when interacting with the fusion center in order to preserve the location privacy. An authentication process based on ECC in the sensing phase operation for the fusion center to authenticate sensing requests.
[28]	2014	Create a secure authentication and communication protocol among CUs and serve the efficiency of less duration time, add more security in the protocols of the MAC layer of the CR	The authentication was mainly based on the use of shared key that is generated by the third trusted party to each CU, through three sequential stages.
[29]	2018	A MAC based energy efficient scheme that can perform under the presence of the SSDF attack	Implements a low overhead symmetric cryptography scheme in order to mitigate the damaging effect on energy caused by the malicious user

3.3 Investigations and Analysis of the Existing Protocol

Research works discussed in the literature review showed different techniques of authentication among CUs. Their approaches varied from each other in terms of the natures of authentication mechanisms, whether it depends on network shared key such as the works in [25,27–29], or depends on digital signature like researches [17,21,23,26]. Moreover, the research works argued and investigated performance in terms of various security issues in CRNs such as packet delay, communication time and proposed solutions for protecting the CRNs environment.

In addition, despite the contributions that have been addressed to upgrade the level of performance and security, the approaches demand a centralized entity in the control phase that manages and controls the security features by generating the required group shared key to be applied for end-users. Consequently, these approaches are inefficient since the centralized entity can be deteriorated by a DoS attack, resulting in compromising the network. For example, in SSMCRN and DSMCRN [24] protocols, the successful, secure communication for a pair of CUs depends entirely on the role of a dedicated server to control the whole communication by providing the required session key for the intended CUs. However, the dedicated server can be a single point of failure if DoS attacks launched on the server. Therefore, enhancing both SSMCRN and DSMCRN is essential to improve the security level by mitigating the aforementioned threat and achieving better performance. Efficient improvements can involve eliminating the use of servers in the control phase of communications and replacing it with a mechanism such as an elliptic curve algorithm.

4 Methodology

Ad Hoc CR network's dynamic features are increasing the complexity of authentication processes among CUs. Therefore, the existing security MAC Protocols in CRNs are being studied and investigated in the literature review. Authors [17,21,23,27,28] had presented some effective approaches for the objectives of ensuring authentication and secure communications among CUs. Analysis and investigations are done thoroughly to the existing approaches conducted by other researchers in securing CRNs, highlighting drawbacks within the existing protocols to achieve reliable and efficient secure communication in CRNs. The methodology of the current scientific research goes through two main stages, the first belonging to explain the design of the proposed architecture of the proposed approach, while the next step is to discuss the changes made within the SSMCRN and DSMCRN protocols for enhancing the security level and improving the performance.

4.1 Architecture and Design of the Proposed Protocol

The whole process and architecture of the proposed effective secure MAC protocol are presented and described in this subsection. The steps shown in Fig. 1 describes the main processes of the communications of the proposed protocol. It consists of three sequential phases, namely the registration, control, and data exchange phases.

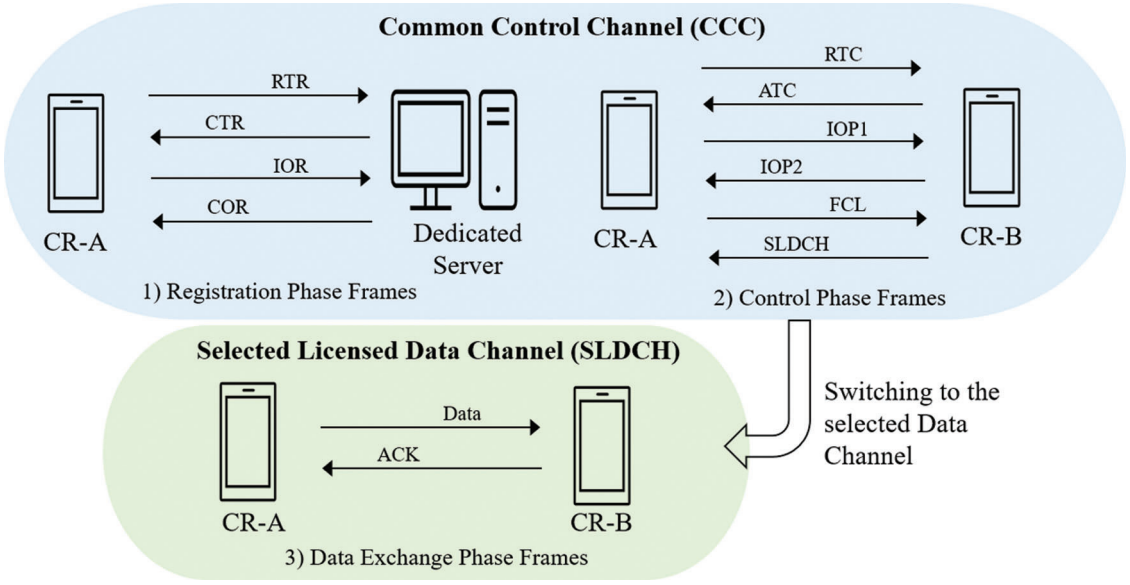

Figure 1: Framework of the proposed effective secure MAC protocol for CRNs

In the first stage, the registration process of the proposed protocol remains the same as described in the SSMCRN protocol [24] and is taking place in the common control channel (CCC). It also has some characteristics such as dedication for the network and aims to obtain a group shared key that indicates a successful registration process with the dedicated server. This key is recognized only by the registered CUs in the network and allows them to communicate in the next phase. the detail of the frames exchange is available in [24].

However, the next stage is the Control phase, where modifications have occurred, and improvements will be implemented in the proposed approach. Therefore, the process of the proposed scheme is shown in Fig. 1 where six frames are involved and exchanged between a pair of CUS before initiating data exchange. The first two frames of the current phase strive to solve the hidden node problem and

exchange the global parameters of the elliptic curve cryptography algorithm (ECC). The next two frames, recognized as information of participation (IoP1 and IoP2), exchange the computed public keys by the participated CUs and enable CUs to generate their session key to be used in the next frames. The last two frames intended to exchange the control information belonging to the sensing results of the idle channels in the Free Channel List (FCL) frame and selecting the best channel for data exchange in the SLDCH frame. Only these two frames of the current phase are protected and confidential using the generated session key to make the negotiated control channels hidden from any malicious users. Accordingly, CUs necessitate switching to the next data phase to exchange data, protected by the generated session key on the previous phase.

Message Authentication Code (MAC) algorithm is involved in each frame to preserve the integrity of the exchanged information. It protects the channel list from being altered and the selected channel from being exposed by an attacker to perform a Jamming attack and make the channel busy.

4.2 The Methodology of the Proposed Contribution

First, to further explain our contribution in this work, we need to understand clearly and explain where the improvements would take place in the existing SSMCRN protocol.

4.2.1 Phases of the Same Procedures in Both Protocols

The first phase of the operation in the protocol which is the registration phase that contains four frames, this process takes place in the common control channel (CCC) when a new CU intends to join a CRN. Mainly, the process in this phase remain the same in the proposed contribution, hence the dedicated server's only job is to register the CU and grant it an ID, and group shared key which is generated by the AES-128 algorithm [24], the group shared key is the primary requirement for authentication purpose. However, although, the last phases in both protocols are slightly the same in which they both exchange control information and data, the sources accountable for session key generation used to encrypt control information and data are different.

4.2.2 Phases of the New Operations in the Proposed Protocol

The improvement and contribution in this domain are taking place in the control phase. Hence the proposed protocol will eliminate the need for the dedicated server due to the aforementioned drawbacks presented in Sections 3.2 and 4.1. Instead, an elliptic curve algorithm is considered to improve the performance of the proposed protocol concerning the desired security requirements. The process is described in details as follows:

Therefore, the registration phase of the proposed protocol's operation is principally going to be the same as in the SSMCRN. The main goal of this procedure is to obtain the CU's ID in the network, and the group shared key that is the primary requirement for authentication purpose and will use in the next control phase to enable CUs to authenticate each other.

However, in the control phase, where the improvement is performed in this work, the pair of involved CUs in the communication will exchange the global parameters of the elliptic curve cryptography algorithm (ECC) to generate their own session key that will be used to encrypt the control information within the FCL and SLDCH frames instead of the server's group shared key that is generated by the dedicated server in SSMCRN protocol. The chosen ECC algorithm in this approach will aid increase the practicality regarding fast performance and network maintenance, less communication time over CCC and fast switching to the SLDCH, improving the throughput, network reliability and efficiency, discharge of the dedicated server.

The last phase in the proposed protocol is the data exchange phase, where both CUs switch to the SLDCH successfully and begin data communications. The exchanged data here is encrypted using the session key generated by the ECC in the control phase.

Next is going to be the implementation stage, followed by the performance evaluation in terms of both communication time and throughput. The obtained results will be compared with the benchmarking protocols known as SSMCRN and DSMCRN since they are close to the proposed protocol.

5 The Implementation and Evaluation of the Proposed Protocol

This section presents the implementation and evaluation processes of the proposed Effective Secure MAC Protocol for CRNs. To obtain the intended successful results, the required security process, including the ECC algorithm, is implemented to generate the session key for a pair of CUs. Other security procedures related to the encryption/decryption and Message Authentication Code (MAC) are performed to ensure the messages' confidentiality and integrity. The section also provides the details of the network parameters considered for evaluating the performance of the proposed protocol for a pair of CUs.

5.1 Experimental Setup

The environment in which this project was taken place to implement is a setup of a computer with an Intel (R) Core (TM) i7-1065G7 CPU @ 1.30 GHz 1.50 GHz, and a RAM of 16.0 GB, 64-bit operating system, ×64-based processor. A windows 10 version 20H2.

5.2 Security Processes

The detail of the security processes of the proposed protocol in the control phase involves the use and exchange of the global parameters of the ECDH algorithm, along with using the MAC algorithm to ensure the integrity of every payload of the exchanged frames among two CUs in the control phase.

5.2.1 Generating Cognitive User's Keys Using ECC Algorithm

The FCL and SLDCH only two frames of the control phase are encrypted/decrypted using the session key derived from the ECC to preserve the confidentiality of control information related to both the list of the free channel and the selected channel. Thus, the implementation process of the ECC algorithm involves generating public/private keys for each CU, and a session key. The following Tab. 2 presents the values produced with generating ECC keys. These values explain the time taken to generate public/private keys for each user in microseconds and the sizes in bits of each key for each CU.

Table 2: Time taken to generate public/private keys of each cognitive user in the control phase

Operation	Generating time	Size (bits)
ECC public and private keys	3385	4128
Session key	504	320

5.2.2 Encryption and Decryption Processes in the Control and Data Exchange Phases

The session key is derived from the ECC algorithm on each side of CUs in the control phase and used to encrypt/decrypt FCL, SLDCH, and data in the communication process of the proposed protocol, the following Tab. 3, gives the results of the encryption, decryption processes in microseconds.

Table 3: Encryption/decryption and MAC generation/verification time in the control and data phases

Frame	Encryption	Cipher size	Decryption	MAC generation	MAC verification
RTC	N/A	N/A	N/A	66	147
ATC	N/A	N/A	N/A	199	135
IoP1	N/A	N/A	N/A	108	161
IoP2	N/A	N/A	N/A	104	189
FCL	332	192	387	78	148
SLDCH	290	192	341	65	93
Data	1481	1692	1100	67	94
ACK	N/A	N/A	N/A	60	91

5.2.3 Generating and Verifying MAC Values over the CCC and Data Channels

Message Authentication Code (MAC) [30] is implemented on every frame in the proposed protocol to preserve the integrity of the payload field and ensure that the messages have not been altered during their transit. The implementation process of the MAC algorithm is conducted, showing the results of time to generate and verify MAC values in microseconds as given in Tab. 3.

5.3 Network Parameters

The network parameters vary and have a direct influence on the protocol performance. To measure the successful communication time process and throughput among CUs of the proposed protocol, the adopted parameters are the same as used in [24] and described in Tab. 4.

Table 4: Network parameters

Parameters	Value	Description
DIFS	50 μs	Distributed interframe space
SIFS	10 μs	Short interframe space
CCC-TR	11 Mbps	CCC transmission rate
DCH-TR	11 Mbps	DCH transmission rate
$T_{DCH}Scan$	5 s	Time of data channels scan
N_{TR}	2	Number of transceivers
PHY layer characteristics	DSSS	Direct-sequence spread spectrum
T_{switch}	10 μs	Time to switch from CCC to SLDCH
CNT_{Window}	32	Contention windows
N_{CCC}	1	Number of common control channel
N_{SLDCH}	10	Number of data channels
N_{CUs}	2	Number of CUs
N_s	1	Number of sensors

5.4 Communication Time

Since the strong security features that the ECC algorithm provides, the proposed protocol is vital to preserving the efficiency of the entire network. This is because of adopting the ECC, enabling each pair of CUs to generate their session key effectively without the need for a centralized entity responsible for providing the required session key for each pair. Therefore, the total time taken to exchange control and data exchange frames for a single pair of CUs in the proposed protocol is 35360.088 ms shown in Fig. 2 below. The time includes; the session key generation on each CU, MAC values generations and verifications, encryptions and decryptions processes. Therefore, the following is the equation of the total time:

$$T = \{T_{DIFS} + T_{RTC} + T_{ATC} + T_{IOP1} + T_{IOP2} + T_{FCL} + T_{SLDCH} + T_{DATA} + T_{ACK} + 3T_{Enc} + 3T_{Dec} + 8T_{GenMAC} + 8T_{VerMAC} + T_{PubPrivCUA} + T_{PubPrivCUB} + 2T_{GenSession} + T_{Switch} + 8 * T_{SIFS}\} \quad (1)$$

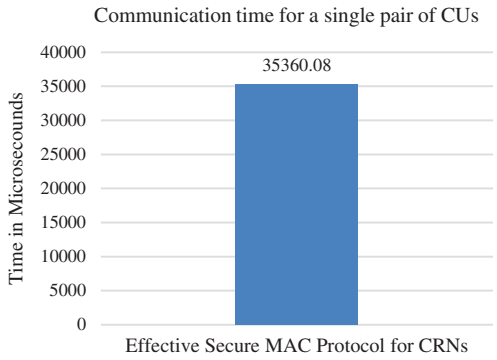

Figure 2: Communication time for successful frames exchange over CCC and SLDCH in the proposed protocol

5.5 Throughput Rate

To evaluate the performance of the proposed Effective Secure MAC Protocol, the throughput must be examined and calculated. Thus, it is the aspect that deals with such evaluations. It is affected by many parameters in the communication processes of the control and data phases. Therefore, the throughput rate of the proposed protocol is measured and presented using Eq. (2) containing several parameters, including the total time T of communications over the CCC and the SLDCH. Other parameters presented in Tab. 5, derived from [24].

$$\eta\alpha \frac{P_{SCCC} * PD * DR * T_X R_X * SDCHs}{T} \quad (2)$$

However, the following Eq. (3) is used and indicating the probability of accessing the CCC successfully (Psccc) that is driven from [24].

$$\text{Psccc} = \left(1 - \frac{1}{CNTWindow}\right)^{N_{CU}-1} \quad (3)$$

Fig. 3 demonstrates the throughput value of the Effective Secure MAC Protocol for Cognitive Radio Networks. The achieved result is 9.0409 to successfully exchange 1500 bytes of data between a pair of CUs.

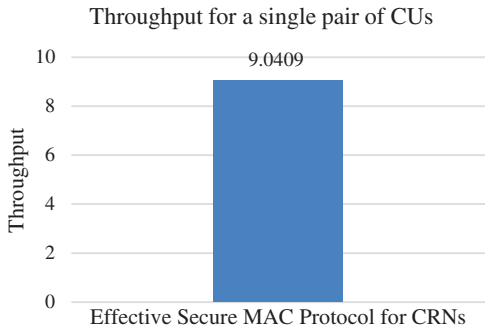

Figure 3: Throughput rate in effective secure MAC protocol

6 Comparison of the Proposed Effective Secure MAC Protocol with Benchmark Protocols

In this section, the proposed Effective Secure MAC Protocol for Cognitive Radio Networks is compared with the existing shared key, and digital signature based secure MAC protocols for Cognitive Radio Networks abbreviated as SSMCRN and DSMCRN in terms of communication time and throughput. Therefore the details of the comparison are explained as follow:

6.1 Communication Time

The total time taken to exchange frames in the Control and Data phases differs in the three protocols shown in Fig. 4. These differences vary based on the type of keys used in each protocol and the dependency on the dedicated server in the SSMCRN and DSMCRN protocols. The values represent a clear view of the huge difference between the proposed protocol and the DSMCRN protocol in particular. Although, both protocols use the same concept of public/private keys. Yet, the efficiency is noticeably high in the proposed protocol as opposed to the DSMCRN. This is the slow operation that the DSMCRN protocol takes to generate and verify the digital signature for each CU. This shows how effective and practical the ECC algorithm is. Despite the common notion about the algorithms that use public-private keys, the ECC is showing great results in terms of less communication time, which is also more practical than the SSMCRN protocol as well despite that it uses a shared key mechanism that is considered faster than the public/private key mechanism, it still has the drawback of dependency on the dedicated server that can affect the whole network if it was under an attack. The results of the time taken to exchange frames in the control and data exchange phases of the proposed protocol indicate that it might achieve high throughput rates since it achieves less communication time and fast switching to the SLDCH to initiate data exchange.

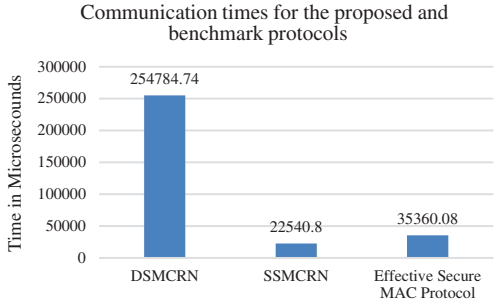

Figure 4: Communication time for successful frames exchange over CCC and SLDCH in the proposed and benchmark protocols

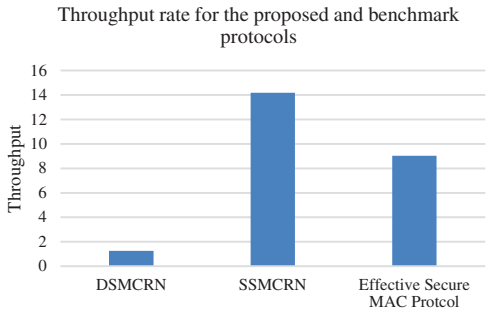

Figure 5: Throughput rate of the proposed effective secure MAC protocol, SSMCRN and DSMCRN

Table 5: Throughput parameters [24]

Parameters	Notations	Relations to the throughput
Number of transceivers	Tx, Rx	Transceivers Tx and Rx are assigned for CCC to monitor network operations and SLDCHs (Increasing the throughput).
Number of LDCH	LDCH	Shows the successful data transmission, increasing LDCH results in decreasing the required time to transfer data (increasing the throughput).
Payload of data	PD	Transmitted data over the SLDCH
Data rate	DR	Data rate for CCC and LDCH set to 11Mbps, increased DR means more data is transmitted, also increasing the network throughput.
Probability of successful access of common control channel	P_{sccc}	The high probability for a CU to successfully access CCC during the control phase, indicates that it's taking less communication time to quickly switch to the SLDCH, which means (increasing the throughput).
Time of communication	T	The more time it takes to communicate over the CCC and the SLDCH the less network throughput rate it will produce.
Parameters	Notations	Relations to the throughput
Number of transceivers	Tx, Rx	Transceivers Tx and Rx are assigned for CCC to monitor network operations and SLDCHs (increasing the throughput).
Number of LDCH	LDCH	Shows the successful data transmission, increasing LDCH results in decreasing the required time to transfer data (increasing the throughput).
Payload of data	PD	Transmitted data over the SLDCH.
Data rate	DR	Data rate for CCC and LDCH set to 11Mbps, increased DR means more data is transmitted, also increasing the network throughput.
N_{CUs}	2	Number of CUs.
N_s	1	Number of sensors.

On the other hand, the communication time of the proposed protocol is longer than the SSMCRN, which means that the proposed protocol takes a longer time in the CCC to exchange the security and control information. The reason why is because the Effective Secure MAC Protocol uses the ECC algorithm, which requires the generation of public/private keys for both users, along with generating the session key as well. In contrast with the SSMCRN protocol, which uses a shared key generated by the AES 128, the ECC session key is much longer than the AES algorithm, clarifying why the proposed protocol takes longer than the SSMCRN. Indeed applying the ECC algorithm effectively maintains the network operation in case the dedicated server was compromised since it enables CUs to generate the necessitated session key to protect the FCL, SLDCH and data exchange. This indicates the ECC algorithm drives the reliability and efficiency of the intended proposed protocol along with a higher security level compared to the symmetric key cryptography.

6.2 Throughput Rate

The following Fig. 5 represents the throughput of the proposed Effective Secure MAC protocol and the other two benchmarks' protocols; DSMCRN and SSMCRN. Generally, the relationship between throughput and communication time is inverse. Thus, it is noticeable that both the proposed protocol and SSMCRN have higher throughput rates than the DSMCRN protocol due to less communication time taken over the CCC, leading to faster switching the SLDCH and initiating the data exchange between a pair of CUs. Nevertheless, the proposed protocol achieved less throughput rate by less than double the SSMCRN protocol's throughput. This is because of adopting the ECC algorithm in the proposed protocol to enhance the reliability, efficiency, and security level of the proposed protocol.

On the other hand, since the DSMCRN protocol incorporates the CUs' digital signatures verified on the authentication server, it demands a longer execution time over the CCC, resulting in slower switching time to the SLDCH. Thus, this mainly affects its throughput rate, which is remarkably dropped compared to both the proposed and SSMCRN protocols.

7 Conclusion and Future work

Cognitive radio networks represent a new dynamic type of smart networks performing efficient utilization of the white spaces. However, it is prone to several attacks that would compromise the communication of participated cognitive users. Preserving the demand for authentication, confidentiality, and integrity lead to successfully secure communication between cognitive users. Therefore, an enhanced and effective secure MAC protocol is presented in this paper to overwhelms the concern of the centralized dedicated server, which can be a single point of failure involved in the control phase of existing DSMCRN and SSMCRN protocols. Accordingly, better network efficiency and reliability are granted since the proposed protocol involved the ECC algorithm that effectively eradicates the need for the dedicated server and performing a distinguished security level of generating the essential session key for a single pair of CUs in the control phase, leading to ensuring the successful confidentiality of the exchanged control information and data.

The proposed protocol is implemented, evaluated and compared with benchmarks for conducting its performance in terms of communication time and throughput. The results confirm remarkable improvements achieved, including less communication time, fast switching to the SLDCH and higher throughput. Moreover, a higher level of protection is positively influenced by eliminating the demand for a dedicated server responsible for granting the required session key within the benchmark protocols.

In future work, the proposed protocol will be deployed for the IoT based on the cognitive radio concept to improve communication within the environment.

Acknowledgement: This project was supported by Taif University Researchers Supporting Project number (TURSP-2020/107), Taif University, Taif, Saudi Arabia.

Funding Statement: Taif University Researchers Supporting Project (TURSP), Taif University, Kingdom of Saudi Arabia under the Grant Number: TURSP-2020/107.

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

[1] C. Cordeiro, K. Challapali, D. Birru and S. Shankar, "IEEE 802.22: The first worldwide wireless standard based on cognitive radios," in *First IEEE Int. Symp. on New Frontiers in Dynamic Spectrum Access Networks, DySPAN 2005*., Baltimore, MD, USA, pp. 328–337, 2005.

[2] K. G. Shin, H. Kim, A. W. Min and A. Kumar, "Cognitive radios for dynamic spectrum access: From concept to reality," *IEEE Wireless Communications*, vol. 17, no. 6, pp. 64–74, 2010.

[3] Y. Arjoune and N. Kaabouch, "A comprehensive survey on spectrum sensing in cognitive radio networks: Recent advances, new challenges, and future research directions," *Sensors*, vol. 19, no. 1, pp. 126, 2019.

[4] D. M. Alias and G. K. Ragesh, "Cognitive radio networks: A survey," in *2016 Int. Conf. on Wireless Communications, Signal Processing and Networking*, Chennai, India, pp. 1981–1986, 2016.

[5] Y. Gu, Q. Pei and H. Li, "Dynamic matching-based spectrum detection in cognitive radio networks," *China Communications*, vol. 16, no. 4, pp. 47–58, 2019.

[6] W. Alhakam, A. Mansour and G. A. Safdar, "Spectrum sharing security and attacks in CRNs: A review," *International Journal of Advanced Computer Science and Applications*, vol. 5, no. 1, pp. 76–87, 2014.

[7] F. Lin, Z. Hu, S. Hou, J. Yu, C. Zhang *et al.,* "Cognitive radio network as wireless sensor network (II): Security consideration," in *Proc. of the 2011 IEEE National Aerospace and Electronics Conf.*, Dayton, OH, USA, pp. 324–328, 2011.

[8] G. Baldini, T. Sturman, A. R. Biswas, R. Leschhorn, G. Godor *et al.,* "Security aspects in software defined radio and cognitive radio networks: A survey and a way ahead," *IEEE Communications Surveys & Tutorials*, vol. 14, no. 2, pp. 355–379, 2012.

[9] L. Gavrilovska, D. Denkovski, V. Rakovic and M. Angjelichinoski, "Medium access control protocols in cognitive radio networks: Overview and general classification," *IEEE Communications Surveys & Tutorials*, vol. 16, no. 4, pp. 2092–2124, 2014.

[10] A. S. Chavan and A. Junnarkar, "Dynamic spectrum sensing method for mobile cognitive radio ad hoc networks," in *2020 Int. Conf. on Emerging Smart Computing and Informatics*, Pune, India, pp. 92–97, 2020.

[11] Z. D. Wang, H. Q. Wang, G. S. Feng, B. Y. Li and X. M. Chen, "Cognitive networks and its layered cognitive architecture," in *2010 Fifth Int. Conf. on Internet Computing for Science and Engineering*, Harbin, China, pp. 145–148, 2010.

[12] Z. Gao, H. Zhu, S. Li, S. Du and X. Li, "Security and privacy of collaborative spectrum sensing in cognitive radio networks," *IEEE Wireless Communications*, vol. 19, no. 6, pp. 106–112, 2012.

[13] H. Elrhareg, M. Ridouani and A. Hayar, "Routing Protocols on cognitive radio networks: Survey," in *2019 IEEE Int. Smart Cities Conf.*, Casablanca, Morocco, pp. 296–302, 2019.

[14] L. Tang and J. Wu, "Research and analysis on cognitive radio network security," *Scientific Research Publishing*, vol. 4, no. 4, pp. 1–7, 2012.

[15] A. He, K. k. Bae , T. R. Newman, J. Gaeddert, K. Kim *et al.,* "A survey of artificial intelligence for cognitive radios," *IEEE Transactions on Vehicular Technology*, vol. 59, no. 4, pp. 1680–1688, 2010.

[16] N. Mishra, S. Srivastava and S. N. Sharan, "Cognitive radio network security threats: A review," in *2019 2nd Int. Conf. on Intelligent Communication and Computational Techniques*, Jaipur, India, pp. 333–338, 2019.

[17] S. Raj and O. P. Sahu, "Security threats and challenges on different protocol layers in cognitive radio networks: An overview," in *2017 Int. Conf. on Innovations in Control, Communication and Information Systems*, Greater Noida, India, pp. 1–5, 2017.

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

[19] J. Gope, P. Dutta, S. Bhadra, S. Das, S. Jana *et al.,* "Analytical study of primary user emulation attack detection techniques in cognitive radio adhoc network," in *2017 IEEE 8th Annual Ubiquitous Computing, Electronics and Mobile Communication Conf.*, New York, NY, USA, pp. 392–395, 2017.

[20] J. N. Soliman, T. A. Mageed and H. M. El-Hennawy, "Taxonomy of security attacks and threats in cognitive radio networks," in *2017 Japan-Africa Conf. on Electronics, Communications and Computers*, Alexandria, Egypt, pp. 127–131, 2017.

[21] B. Wang and K. J. R. Liu, "Advances in cognitive radio networks: A survey," *IEEE Journal of Selected Topics in Signal Processing*, vol. 5, no. 1, pp. 5–23, 2011.

[22] W. Huayi and B. Baohua, "A Secure protocol in MAC layer of cognitive radio networks," in *2019 Int. Conf. on Computer, Information and Telecommunication Systems*, Beijing, China, pp. 1–4, 2019.

[23] J. N. Soliman, T. A. Mageed and H. M. El-Hennawy, "Digital signature and authentication mechanisms using new customized hash function for cognitive radio networks," in *2017 12th Int. Conf. on Computer Engineering and Systems*, Cairo, Egypt, pp. 175–181, 2017.

[24] W. Alhakami, "Secure MAC protocols for cognitive radio networks," Ph.D. dissertation, University of Bedfordshire, pp. 1–235, 2016.

[25] W. Alhakami, A. Mansour, G. A. Safdar and S. Albermany, "A secure MAC protocol for cognitive radio networks (SMCRN)," in *2013 Science and Information Conf.*, London, UK, pp. 1–8, 2013.

[26] H. Lai, L. Xu and Y. Zeng, "An efficient location privacy-preserving authentication scheme for cooperative spectrum sensing," *IEEE Access*, vol. 8, pp. 163472–163482, 2020.

[27] M. Khasawneh and A. Agarwal, "A secure and efficient authentication mechanism applied to cognitive radio networks," *IEEE Access*, vol. 5, pp. 15597–15608, 2017.

[28] W. Alhakami, A. Mansour and G. A. Safdar, "Shared-key based secure MAC protocol for CRNs," in *2014 Eighth Int. Conf. on Next Generation Mobile Apps, Services and Technologies*, Oxford, UK, pp. 266–271, 2014.

[29] J. Dai, J. Liu, C. Pan, J. Wang, C. Cheng *et al.,* "MAC based energy efficiency in cooperative cognitive radio network in the presence of malicious users," *IEEE Access*, vol. 6, pp. 5666–5677, 2018.

[30] J. V. Espoo and V. N. Helsinki, "MESSAGE AUTHENTICATION," (U.S. Patent No. 10/476,988, United States, pp. 1–15, 2005.