IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received May 26, 2017, accepted June 27, 2017, date of publication July 4, 2017, date of current version August 22, 2017.

Digital Object Identifier 10.1109/ACCESS.2017.2723322

A Secure and Efficient Authentication Mechanism Applied to Cognitive Radio Networks

MAHMOUD KHASAWNEH AND ANJALI AGARWAL, (Senior Member, IEEE)
Department of Electrical and Computer Engineering, Concordia University, Montreal, QC H3G 1M8, Canada
Corresponding author: Mahmoud Khasawneh (khasawneh87@yahoo.com)

ABSTRACT Cognitive radio (CR) has been introduced to accommodate the steady increment in the spectrum demand. Wireless security in CR network (CRN) is a challenging technical area due to the dynamic and unique characteristics of CRNs. As a cognitive node can dynamically join or leave the spectrum, providing secure communication becomes problematic and requires more investigation. Authentication is a primary security property in wireless networks, wherein the identity of a cognitive node is verified before providing access to available resources. In this paper, a two-level authentication scheme for communication in a CRN is proposed. Before joining the network, a CR node is validated by obtaining security credentials from an authorized point. The proposed scheme relies on public- and symmetric-key cryptography, instead of using a digital signature-based approach. It encrypts data between the communicating nodes in order to improve network security in terms of resource availability and accessibility. This mitigates attacks such as *reflection attack*, *denial of service attack*, and *man-in-the-middle attack*. The scheme has been evaluated and verified in terms of security functionality, its correctness, and the performance, which shows less computation and communication requirements.

INDEX TERMS Authentication, cognitive radio, security, symmetric key, cryptography.

I. INTRODUCTION

Recently, cognitive radio (CR) has become one of the most commonly studied techniques in the field of wireless networks [1]. Currently, the conventional spectrum management approach is widely applied by regulators all over the world, wherein the regulators assign the spectrum frequency bands locally to service providers for large geographical ranges and for long periods of time. Then, each service provider manages its frequency bands by defining its users, their rights, and specifying the regulations that control the communication over its channels. Although these regulations intend to enhance the spectrum usage, they can lead to a spectrum scarcity problem. A service provider sells the spectrum in the form of bandwidth to its end users, referred as primary users (PUs) [2]. These PUs, which own the spectrum for a long term, can resell their unused spectrum to other users known as secondary users (SUs).

Cognitive radio networks differ from other wireless networks. Some reliability issues are unique to CRN, such as its high sensitivity to weak primary signals, its unknown primary receiver location, its tight synchronization requirement in centralized cognitive radio networks, and its lack of a common control channel [3].

The radio technology itself is vulnerable to attacks, as any radio frequency can be blocked or jammed if a transmitter sends a signal at the same frequency with enough power. As any other type of wireless networks, CRNs are vulnerable to many security attacks [4], such as Denial of Service attack, Man-in-the-Middle attack, and Reflection attack.

Unlicensed users can use the white bands of the spectrum in the absence of licensed users. There is no control over the behavior of these unlicensed users, which threatens the security of the licensed users. A node can use the vulnerability of CRN reliability and the absence of control to attack the different layers of the communication protocol.

There are many concepts that should be applied to satisfy a secure communication among CRNs, which are referred to as security requirements: confidentiality, integrity, availability and authentication [5].

Confidentiality serves to protect information in order to prevent unauthorized access to the system and/or individuals information. Data confidentiality is an essential requirement in CRNs in order to protect the privacy of the data owner's (PU or SU) personal information including bank storing credit and balance information [6]. Moreover, since radio is the communication medium in CRNs, which makes it open for access and more vulnerable to attacks, confidentiality should be guaranteed for each connection.

Integrity is the security requirement of ensuring that information will not be accidentally or maliciously altered

2169-3536 © 2017 IEEE. Translations and content mining are permitted for academic research only.
Personal use is also permitted, but republication/redistribution requires IEEE permission.
See http://www.ieee.org/publications_standards/publications/rights/index.html for more information.

or destroyed. It means that data is transmitted from the source to the destination without alteration [7]. The message can only be altered by the sender without detection by other nodes. Integrity protects against unauthorized data creation, alteration or destruction. If a corrupted message is accepted, then this would be detected as a violation of the integrity property [8].

Availability allows the network users to use the network for their own transmissions and to keep track of the traffic over the network [6]. In CRN, when PUs are not using their spectrum channels, other users (SUs) can use these channels. However, once a PU wants to use its channels again, all SUs have to leave immediately to make the channels available.

Authentication is the verification process of the claimed identity of a user [9]. It is a primary security requirement since the other requirements first require propoer authentication. In CRN, each node has to authenticate itself before it can use the available spectrum channels. One access point takes care of the authentication process wherein all SUs identify themselves to the access point.

In this paper, our main focus is the authentication process in CRNs in order to ensure secure communication. As mentioned previously, the authentication process is considered to be the primary security requirement in wireless networks. The protocol scope is within CRNs as the cognitive capability provides more dynamicity to the communicating nodes in the network, which makes the authentication process easier to implement. Moreover, we authenticate the users that do not have a permession to access the network resources, which differs from other networks that only authenticate and grant licensed users access to the network resources. We propose a two-level authentication scheme to validate the cognitive node and its user. The scheme takes place on different layers (i.e. physical, data link, and network) to authenticate the node, and on the application layer to authenticate the node's user. The proposed scheme aims to provide additional security in CRN networks to ensure that the network resources are available and permit access to these resources for authenticated nodes only. Moreover, as the proposed authentication scheme is completed over different layers, it would mitigate different potential attacks such as a reflection attack, a denial of service attack, and a man-in-the-middle attack.

The rest of this paper is organized into five more sections. In Section II, a literature review is conducted. In Section III, the authentication scheme will be explained. The proposed model is evaluated and verified in detail in Section IV. Section V presents the scheme's performance evaluation results that show the efficiency of the proposed model compared to other models. Lastly, we conclude this paper in Section VI.

II. RELATED WORK

Authentication process has been researched in all kinds of wireless networks with different solutions proposed. In [10], Wong et al. proposed a dynamic user authentication scheme in Wireless Sensor Networks (WSN). It allows legitimate users to request the sensor data from any of the sensor nodes by imposing less computational load. This scheme claimed that it is secure against replay and forgery attacks. However, Tseng et al. in [11] proved that the scheme proposed in [10] is vulnerable to replay and forgery attacks and proposed an authentication mechanism to overcome the drawbacks of [10]. Han et al. in [12] proposed a distributed node authentication model wherein all the network nodes are involved in the authentication process as an authenticator. The main drawback of this scheme is the increased computational cost and communication overhead. Another authentication scheme is proposed by Zhu et al. in [13], where each node generates a one-way key chain and sends the commitment of it to its neighbors. If a node wants to send a message to its neighbors, it attaches the next authorization key from its key chain to the message. The receiving node can verify the validation of the key based on the commitment it has already received. The main drawback of this scheme is that it does not mitigate attacks from nodes which are already part of the networ; since the adversary knows the node's authorization key. Ning et al. in [14] have proposed an authentication scheme that uses one-way-key-chain to filter false messages sent between the access point and the sensor nodes. However, the main disadvantage of this scheme is that it uses signature-based authentication, which requires synchronization and periodic broadcasting between the access points and the sensor nodes.

Tan et al. in [15] proposed an approach to strengthen the accuracy of the spectrum sensing process, in which each primary user has to add its unique signature to its signal. No node can emulate a PU during the sensing process, as it cannot provide the PU's signature, and therefore the PUE attack is mitigated. Furthermore, the authors claim that the authentication cannot be done on layers other than the physical layer as nodes might not deploy similar protocols at higher layers and therefore, the authentication messages would not be understood. However, in CRN, nodes are capable of understanding messages on different layers as they run similar software, which can translate messages in a way that each node can understand it. Kim in [16] proposed an authentication scheme that uses the node's location information as a key factor to authenticate the cognitive nodes by a base station. However, it cannot be applied without the integration of the extensible authentication protocol (EAP).

Parvin et al. in [17]–[19] have proposed a digital signature-based authentication scheme, which takes place on the physical and data link layers, to find and permit the trusted users existing in CRNs to access the spectrum. Despite the importance of this work to secure the communication in CRN, its performance evaluation shows that the message transfer with a digital signature takes a long time in comparison to a normal message transfer without a digital signature. In [20] a mutual authentication protocol based on a timestamp in Wireless Sensor Networks (WSNs), which generates a new session key for each session, is proposed.

There are many limitations in previous authentication approaches. First, at they take a long time to complete the authentication process. Second, they rely on digital signature cryptography and more messages are transferred during the authentication process. Last, the other approaches focused more on authenticating the spectrum usage and/or the joining node. Our proposed authentication scheme differs from other authentication schemes proposed in the literature in many aspects, as following:

- It is a two-level authentication, wherein the authentication process is done by two different entities (fusion center (FC) and cluster head (CH) defined later in Section III) consecutively, and the joining node can gain access to the network resources only after it has been verified by both the entities.
- It utilizes the advantages of public and symmetric key cryptography approaches to encrypt messages sent between the joining node and the authenticating entities (both FC and CH), while other schemes apply the digital signature-based approach which requires synchronization and periodic broadcasting that takes a longer execution time.
- It authenticates the spectrum usage and the joining node in addetion to the user. Other authentication schemes focused more on authenticating the spectrum usage and/or the joining node; however, the user of the joining node needs also to be authenticated to ensure whether it is a legitimate user.
- The authentication process in our proposed scheme is carried over different layers (physical, data link, network, and application), while the other authentication schemes are done on the physical and data link layers only. Authentication on different layers strengthens the authentication process.
- It mitigates different attacks that target the different layers such as the reflection attack, the denial of service attack, and the man-in-the-middle attack, which can occur after the spectrum sensing phase is done. While other authentication schemes focus more on mitigating the Primary User Emulation (PUE) attack only, which takes place during the spectrum sensing phase.
- It is specific to CRNs, as an attacker (misbehaving SU) may emulate a primary user's signal to lure other secondary users. Therefore, a secure authentication algorithm is needed that can determine if a signal sent over the network is a primary user's signal or an attacker's signal. A unique challenge in addressing this problem is that the Federal Communications Commission (FCC) prohibits authentication or any modification to primary users after they buy the spectrum license [21]. Consequently, existing cryptographic techniques cannot be used directly.

We verify the correctness of our proposed authentication scheme by using two different formal verification methods. The first method is Burrows, Abadi, and Needham (BAN) logic [22], which is a formal logic technique that is generally applied to judge protocols and encryption models. It is designed specifically for authentication protocols to prove that a protocol can reach its expected goals and has many advantages such as its simplicity and ease of use. These characteristics make it a good choice to verify our proposed authentication scheme. The second method is an automated validation tool namely Scyther [23] that shows how safe the proposed scheme is from potential well-known attacks. It is a tool for the formal analysis of security protocols. It provides an explicit, modular, and formal language to express protocols and their security features [23].

III. THE PROPOSED APPROACH

In this section, our two-level secure authentication scheme is explained. It is based on public and symmetric key cryptography, which reduces the number of cryptographic operations and the authentication time needed to complete the authentication process.

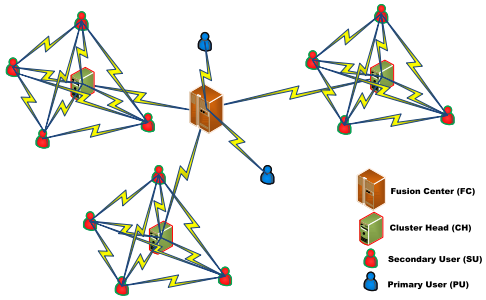

FIGURE 1. System model.

A. PREFACE

Figure 1 illustrates our system, which is a network that has M SUs divided into K different clusters based on their geographical locations wherein each cluster has a unique identifier (Cluster ID) within the network. A Fusion Center (FC) controls the traffic over the network. In each cluster, one node is chosen by the FC as a cluster head (CH). Any secondary user that wants to join the network has to be authenticated before it can use the network. Authentication is the process of validating the identity of the new or returning node(s) to the network. The joining node has to pass through the authentication process at the fusion center level and at the cluster head level.

In order to guarantee security in CRNs, we utilize two different methodologies which are: public-key-infrastructure-based and symmetric-key cryptography. To make the communication of the current nodes secure, we propose that the communication between the network nodes is completed by utilizing the public-key cryptography. This will secure the communication until a symmetric key is shared among the communicating nodes, which is used to encrypt and decrypt messages onwards. Symmetric-key cryptography has many advantages that make it a good choice to use, such as its straightforwardness, its less memory occupation, its less

memory use, and its less power utilization. The symmetric key will be assigned to each node during the authentication process. Each node uses the same symmetric key for encoding and decoding the messages after it is shared amongst themselves. When a node sends a message to another node in the network, this message will be encrypted with the symmetric key. Meanwhile, the receiver decrypts this message by using the same symmetric key.

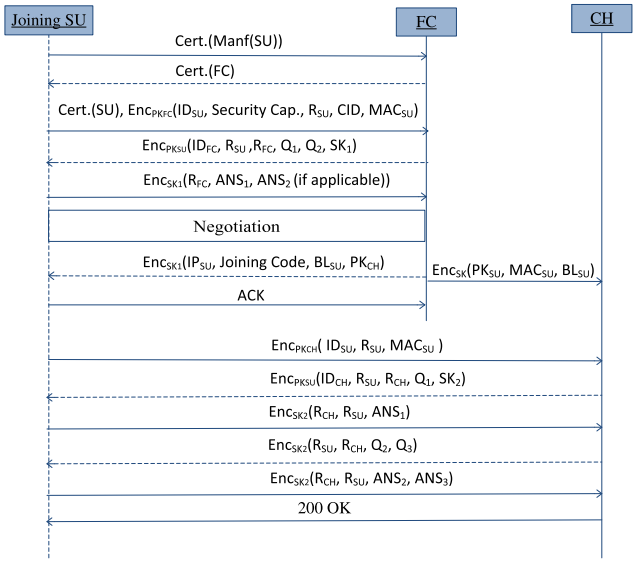

FIGURE 2. The sequence diagram of the proposed scheme.

B. SCHEME DESCRIPTION

The proposed authentication scheme aims to authenticate the node (device) and its user as well as the spectrum usage. It works at two different levels, which are the FC's level and the CH's level. The joining node has to correctly pass over the proposed two levels of authentication in order to be admitted as a part of the CRN. The message sequence of the proposed authentication scheme is illustrated in Figure 2. We define the terms that will be used in our proposed authentication model as follows:

- X: represents one of the system entities which are FC, CH, or SU.
- Cert.(Manf(X)): the manufacturer's certificate of entity X.
- PK_X: the public key of entity X.
- ID_X: the logical identifier of entity X.
- MAC_X : the hardware address of entity X.
- Cert.(SU): the manufacturing certificate of entity SU, which contains ID_X, MAC_{SU}, and PK_{SU}.
- Cert.(FC): the manufacturing certificate of entity FC, which contains ID_{FC}, MAC_{FC}, and PK_{FC}.
- ENC(Info.): all info. is encrypted before sending it.
- R: a random number (Nonce) generated by the sender and sent with each message to track the messages and to correlate with their response messages.
- CID: connection ID.
- Symmetric Key: a key used for encryption and decryption by the communicating nodes (FC, SU, and CH), SK_1 between the FC and SU, SK_2 between SU and the CH.
- Joining Code: generated by the FC. The joining code is unique within the cluster and is known by the nodes of the cluster. This joining code will be used to determine if this joining node is known to other cluster nodes.
- Security Capabilities: the features or properties that a node supports to make a secure communication with other nodes such as encryption/decryption protocol, message integrity code and key management cryptography algorithm.
- Belief Level (BL): describes the level of reliability of a node to participate in data transmission over the network.

A node's certificate is validated through a server node, S, known to all the nodes. The server S grants a certificate to each node after it has been manufactured. The node's certificate includes its logic identifier, its MAC address and a pair of its public/private keys. As each node's certificate is signed by the server's key, each node contacts the server S to validate other nodes' certificate(s). During the certificate validation, each node gets all the node information from the server S except the node's private key which is not shared with any other node in the network. After users' certificates have been validated, all messages exchanged between the FC/CH and the joining node cannot be accessed by a listening adversary as the receiving node can easily determine if the received message was sent from an intruder or not, based on the node's ID and its public key.

TABLE 1. Questions to the joining node.

Question		Joining Node Status	Asked by
Q_1	What is(are) the cluster(s) ID that you want to join?	New or Returning	FC & CH
Q_2	What is the joining code of the cluster(s) that you want to join?	Returning	FC & CH
Q_3	What is your BL?	New or Returning	CH

During the authentication process, the authenticating node (i.e. FC or CH) asks the joining node up to three different questions as shown in Table 1. Answering these questions correctly by the joining node leads to the successful authentication of this joining node. During the first level of authentication, the FC asks the joining node Question 1 (Q_1) and Question 2 (Q_2) to check what information this node has about the joining cluster. If the joining node is a returning node to the same cluster, it has to answer the two questions correctly. However, if the node is a returning node, but to a different cluster or the node is completely a new node, it answers Q_1 only. The FC keeps track of all joined nodes by storing their MAC address in a database that is used to

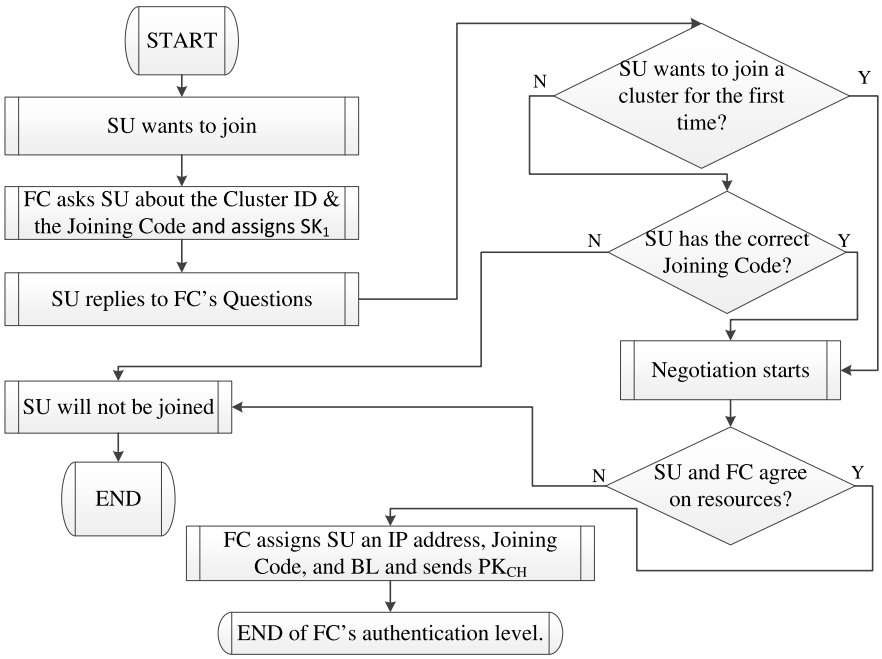

FIGURE 3. Flow chart for authentication at the FC level.

determine if a joining node is a new node or a returning node. During the second level of authentication, the CH asks the joining node all three questions as it should have the answers to all these questions as long as it has correctly passed the FC's level of authentication.

Each SU performs spectrum sensing to determine if any white spectrum channels are available for use. If yes, SU contacts the cluster(s) nodes within its range, in order to get their cluster IDs, which are required during the authentication process.

1) FIRST LEVEL OF AUTHENTICATION AT FUSION CENTER

The FC's authentication level starts by validating the nodes' certificate wherein the certificates of the joining node and the authenticating node are validated through the server S. During the certificate validation, the joining node (SU) sends its manufacturer certificate (Cert.(Manf (SU))) to the FC, which accepts nodes from a predefined manufacturers' list to access the network. If this joining node is from a known manufacturer, the FC replies to SU by sending its own certificate (Cert.(FC)). Then, SU sends its own certificate (Cert(SU)) as well as a message ($ENC_{PKFC}()$), encrypted with PK_{FC}, that contains its ID (ID_{SU}), its security capabilities, a random number (Nonce) R_{SU}, a connection ID (CID), and its MAC address. A MAC address is used because it is unique for each node at the authentication layer. The FC sends a message ($ENC_{PKSU}()$), encrypted with PK_{SU}, to the joining SU, which contains its ID (ID_{FC}), symmetric key SK_1 used to encrypt/decrypt the messages exchanged from now on, a random nonce (R_{FC}) connected with the received R_{SU}, and questions (Q_1 and Q_2). The purpose of these questions is to ensure that this joining node has enough information about the cluster(s) that it wants to join.

If the joining node is a new node or a returning node to a different cluster, Q_1 will be answered only by sending ANS_1, which includes all cluster(s) ID(s) that SU receives from nodes within its range. However, if the joining node is a returning node to the same cluster that it was part of during the last connection time, it answers both Q_1 and Q_2 by sending ANS_1 and ANS_2. If a returning node to the same cluster fails to provide the FC with the joining code, it will not be admitted. The joining SU replies to Q_1 and Q_2 by sending ANS_1 and ANS_2 encrypted with the symmetric key SK_1. Upon the success of answering Q_1 and Q_2 (if applicable), the resource negotiation phase starts, in which the joining SU sends its QoS requirements to the FC. The FC takes the responsibility of determining if the desired cluster can provide the QoS requirements or not.

The negotiation phase ends with either an agreement or a disagreement between the joining SU and the FC. If both do not agree on resources, SU will not be joined. If both of them agree on resources, the FC assigns an IP address to this node, provides it with the cluster joining code, calculates a value called belief level, and prepares the public key of the CH, PK_{CH}. The belief level describes the level of reliability of this node to participate in data transmission over the network. The public key of the CH is used in the second level of authentication at the CH. The node's IP address, the node's belief level, the cluster head's public key, and the cluster's joining code are encrypted in one message and sent to the joining node. Meanwhile, the FC sends the node's MAC address, the node's belief level, and the node's public key PK_{SU} to the CH. These parameters are sent in an encrypted message, as the FC and the CH communicate over a secure control channel. Figure 3 illustrates the flow chart of the FC level authentication.

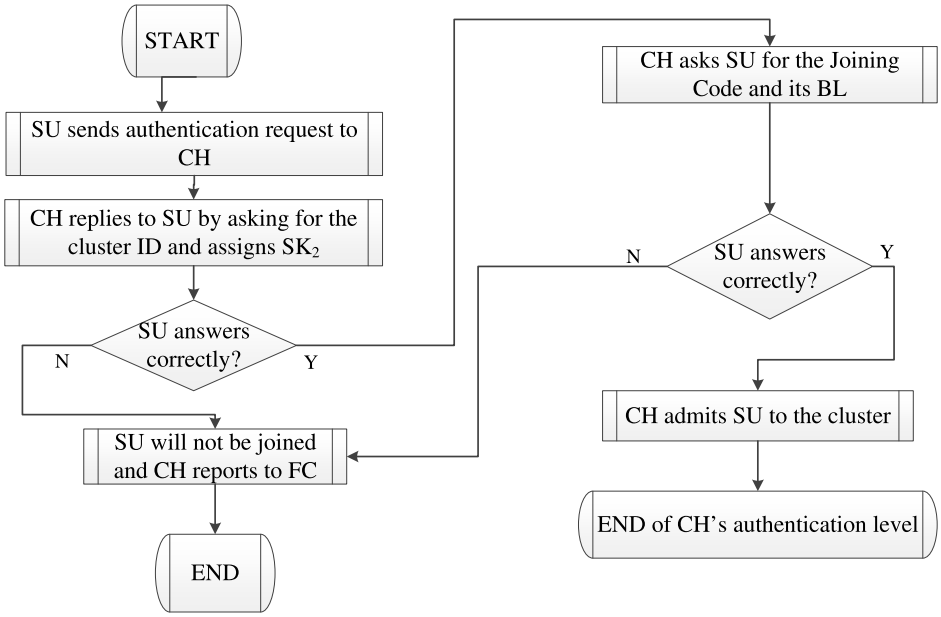

FIGURE 4. Flow chart for authentication at the CH level.

2) SECOND LEVEL OF AUTHENTICATION AT CLUSTER HEAD

The joining SU starts the second level of authentication by sending a message ($ENC_{PKCH}()$), encrypted with the already known CH's public key, to the cluster head. This encrypted message contains the joining node's public key PK_{SU}, its MAC address, and a random number R_{SU}. The CH now wants to authenticate the user of this joining node by asking three questions. First, the CH sends ($ENC_{PKSU}()$), an encrypted message with the joining node's public key. In this messgae, CH asks the joining SU about the cluster ID, and sends the symmetric key, SK_2, that will be used to encrypt/decrypt the messages from now on. The joining SU replies by sending its answer encrypted with the SK_2.

If the joining SU answers correctly, the CH sends an encrypted message with the SK_2 asking the joining SU Q_2 about the cluster's joining code and Q_3 about its BL. The joining SU replies by sending its answers (ANS_2 and ANS_3) encrypted with the SK_2. If the joining SU answers correctly, the CH admits the joining SU to be part of the cluster. The SU can now join the cluster and can start transmitting data with the other cluster nodes. If the joining node fails to answer any of these three questions, it will not be admitted and the CH sends a report to the FC. Figure 4 illustrates the flow chart of the CH level authentication.

Each message sent between the joining node and the authenticating node contains their random (nonce) numbers which are used to synchronize messages and to prevent any intruder from eavesdropping on the messages exchanged between the communicating nodes. On the other hand, each node's ID is sent encrypted once the node sends its first message to the other communicating party. The message receiver validates the sender's ID by extracting the sender's ID from the sender's certificate sent earlier, and compares it with the received one. This Validation prevents the messages exchanged between the communicating nodes from being accessed by an intruder; and therefore, improving the network security.

IV. SCHEME EVALUATION

A. SCHEME VERIFICATION

We verify the correctness of our proposed authentication scheme by using two different formal verification methods which are BAN logic and Scyther verification tool.

1) VERIFICATION THROUGH BAN LOGIC

In BAN logic, all messages sent between the two communicating nodes are formulated according to the BAN logic format and then BAN logic axioms and messages' analysis are applied to these messages to conclude if the protocol meets its desired objectives or not.

The axioms used to prove the correctness of an authentication mechanism are as follows:

We assume that there are two network agents (P and Q), a message (X) is exchanged between the network agents. Message (X) is encrypted by an encryption key (K). The definitions and their implications are below:

- P believes X: P acts as if X is true, and may assert X in other messages.
- P said X: At one time, P transmitted and believed message X, although P might no longer believe X.

- P sees X: P receives message X, and can read and repeat X.
- fresh(X): X has not previously been sent in any message.

We define the terms used through the verification process in our authentication mechanism as follows:

- SU, FC, and CH: are the network agents.
- S: is a third party known to all nodes similar to service provider base station.
- (Info.): is the message encrypted.
- PK_{FC}: is the public key of entity FC.
- PK_{SU}: is the public key of entity SU.
- PK_{CH}: is the public key of entity CH.
- PK_S: is the public key of the server S and known to SU and FC which grants certificates to each node.
- ID_{FC}: is the logical identifier of entity FC.
- ID_{SU}: is the logical identifier of entity SU.
- ID_{CH}: is the logical identifier of entity CH.
- R_{FC}: is a random number (nonce) generated by FC.
- R_{SU}: is a random number (nonce) generated by SU.
- $SU \overset{SK_1}{\Leftrightarrow} FC$: is the symmetric key that SU and FC agree during the FC level authentication
- $SU \overset{SK_2}{\Leftrightarrow} CH$: is the symmetric key that SU and CH agree during the CH level authentication

a: AUTHENTICATION AT FC LEVEL

We can represent the goals of the FC level authentication according to BAN logic as following:

$$SU\ believes SU \overset{SK_1}{\Leftrightarrow} FC$$
$$FC\ believes FC \overset{SK_1}{\Leftrightarrow} SU$$

Here are the idealized messages of the FC's level authentication, note that we omit the messages and the parts of messages which do not affect the sender and receiver identities.

$$MSG1 : FC \rightarrow SU : ENC_{PK_S}(MAC_{FC} \overset{PK_{FC}}{\longrightarrow} FC).$$
$$MSG2 : SU \rightarrow FC : ENC_{PK_S}(MAC_{SU} \overset{PK_{SU}}{\longrightarrow} SU), ENC_{PK_{FC}}(ID_{SU}, R_{SU}, MAC_{SU}).$$
$$MSG3 : FC \rightarrow SU : ENC_{PK_{SU}}(ID_{FC}, R_{SU}, R_{FC}, Q_1, Q_2, SU \overset{SK_1}{\Leftrightarrow} FC).$$
$$MSG4 : SU \rightarrow FC : ENC_{SK_1}(R_{FC}, ANS_1, ANS_2).$$

Here are the assumptions:

$$SU\ believes \overset{PK_{SU}}{\longrightarrow} SU$$
$$FC\ believes \overset{PK_{FC}}{\longrightarrow} FC$$
$$SU\ believes \overset{PK_S}{\longrightarrow} S$$
$$FC\ believes \overset{PK_S}{\longrightarrow} S$$
$$SU\ believes fresh\ (R_{SU})$$
$$FC\ believes fresh\ (R_{FC})$$
$$SU\ believes\ FC\ controls (SU \overset{SK_1}{\Leftrightarrow} FC)$$
$$FC\ believes\ FC\ controls (SU \overset{SK_1}{\Leftrightarrow} FC)$$

We apply the axioms of BAN logic on each message.

On message 1:

$SU\ sees\ (MAC_{FC}, \overset{PK_{FC}}{\longrightarrow} FC)$ **and** $SU\ believes \overset{PK_S}{\longrightarrow} S$, **therefore** $SU\ believes\ S\ said\ (MAC_{FC}, \overset{PK_{FC}}{\longrightarrow} FC)$. **So**, $SU\ believes\ S\ believes\ (MAC_{FC}, \overset{PK_{FC}}{\longrightarrow} FC)$, **which means** $SU\ believes\ S\ controls\ (MAC_{FC}, \overset{PK_{FC}}{\longrightarrow} FC)$, **which results in** $SU\ believes\ (MAC_{FC}, \overset{PK_{FC}}{\longrightarrow} FC)$.

For simplicity we consider the part that is related to the public key cryptography, hence $SU\ believes \overset{PK_{FC}}{\longrightarrow} FC$.

On message 2:

We start by considering the first part of message 2, which is $ENC_{PK_S}((MAC_{SU}, \overset{PK_{SU}}{\longrightarrow} SU))$. $FC\ sees\ (MAC_{SU}, \overset{PK_{SU}}{\longrightarrow} SU)$ **and** $FC\ believes \overset{PK_S}{\longrightarrow} S$, **therefore** $FC\ believes\ S\ said\ (MAC_{SU}, \overset{PK_{SU}}{\longrightarrow} SU)$. **So**, $FC\ believes\ S\ believes\ (MAC_{SU}, \overset{PK_{SU}}{\longrightarrow} SU)$, **which means** $FC\ believes\ S\ controls\ (MAC_{SU}, \overset{PK_{SU}}{\longrightarrow} SU)$, **which results in** $FC\ believes\ (MAC_{SU}, \overset{PK_{SU}}{\longrightarrow} SU)$.

For simplicity we consider the part that is related to the public key cryptography, hence FC believes $\overset{PK_{SU}}{\longrightarrow} SU$.

We next consider the second part of message 2, which is $ENC_{PK_FC}(ID_{SU}, R_{SU}, MAC_{SU})$. The only deduction that we obtain is $FC\ sees\ (ID_{SU}, R_{SU}, MAC_{SU})$.

On message 3:

$SU\ sees\ (ID_{FC}, R_{SU}, R_{FC}, Q_1, Q_2, SU \overset{SK_1}{\Leftrightarrow} FC)$, **but** $SU\ believes\ fresh\ (R_{SU})$, **therefore** $SU\ believes\ fresh\ (ID_{FC}, R_{SU}, R_{FC}, Q_1, Q_2, SU \overset{SK_1}{\Leftrightarrow} FC)$. $SU\ believes \overset{PK_{FC}}{\longrightarrow} FC$, **and** $SU\ sees\ (ID_{FC}, R_{SU}, R_{FC}, Q_1, Q_2, SU \overset{SK_1}{\Leftrightarrow} FC)$, **therefore** $SU\ believes\ FC\ said\ (ID_{FC}, R_{SU}, R_{FC}, Q_1, Q_2, SU \overset{SK_1}{\Leftrightarrow} FC)$. With the previous derivation **we conclude that** $SU\ believes\ FC\ believes\ (ID_{FC}, R_{SU}, R_{FC}, Q_1, Q_2, SU \overset{SK_1}{\Leftrightarrow} FC)$, **and with the assumption** $SU\ believes\ FC\ controls\ (SU \overset{SK_1}{\Leftrightarrow} FC)$, **we find that** $SU\ believes\ (ID_{FC}, R_{SU}, R_{FC}, Q_1, Q_2, SU \overset{SK_1}{\Leftrightarrow} FC)$, **which means** $SU\ believes\ SU \overset{SK_1}{\Leftrightarrow} FC$. (a)

On message 4:

$FC\ sees\ (R_{FC}, ANS_1, ANS_2)$ and then compares the received R_{FC} with the sent R_{FC}. If both are equal, it means FC ensures that SU has received SK_1.

Therefore, $FC\ believes\ SU\ believes\ (SU \overset{SK_1}{\Leftrightarrow} FC)$, **and with the assumption** $FC\ believes\ FC\ controls\ (SU \overset{SK_1}{\Leftrightarrow} FC)$, **we find that** $FC\ believes\ (SU \overset{SK_1}{\Leftrightarrow} FC)$. (b)

Derivations (a) and (b) are the objectives of our proposed authentication scheme on the FC's level.

b: AUTHENTICATION AT CH LEVEL

The authentication on the CH's level aims to validate the identity of the SU, i.e. the CH ensures that the user of the CR node is a legitimate user already authenticated by the FC and has got the information needed. This authentication level follows the question and answer method wherein the CH asks the SU for some information and SU replies with the answers.

Failing in answering any of these questions results in not accepting the node in the network and a report will be sent to the FC.

The messages exchanged between the CH and the SU are:

$$MSG1 : SU \rightarrow CH : ENC_{PK_{CH}}(ID_{SU}, R_{SU}, MAC_{SU}).$$
$$MSG2 : CH \rightarrow SU : ENC_{PK_{SU}}(ID_{CH}, R_{SU}, R_{CH}, Q_1, SU \overset{SK_2}{\Leftrightarrow} CH).$$
$$MSG3 : SU \rightarrow CH : ENC_{SK_2}(R_{CH}, R_{SU}, ANS_1).$$
$$MSG4 : CH \rightarrow SU : ENC_{SK_2}(R_{SU}, R_{CH}, Q_2, Q_3).$$
$$MSG5 : SU \rightarrow CH : ENC_{SK_2}(R_{CH}, R_{SU}, ANS_2, ANS_3).$$

According to BAN logic the goals of the CH authentication level are:

$$SU\ believes SU \overset{SK_2}{\Leftrightarrow} CH$$
$$CH\ believes CH \overset{SK_2}{\Leftrightarrow} SU$$

Note that CH encrypts question 1 in message 2 by the public key of SU while question 2 and question 3 in messages 4 and 6 are encrypted with the symmetric key SK_2 upon the key agreement between the CH and SU that occurs in message 3. Therefore to verify the correctness of this authentication level, we need to apply BAN logic to the first three messages only.

Here are the assumptions:

$$SU\ believes \overset{PK_{SU}}{\longrightarrow} SU$$
$$CH\ believes \overset{PK_{CH}}{\longrightarrow} CH$$
$$SU\ believes \overset{PK_{CH}}{\longrightarrow} CH$$
$$CH\ believes fresh\ (R_{SU})$$
$$FC\ believes\ fresh(R_{CH})$$
$$SU\ believes\ CH\ controls (SU \overset{SK_2}{\Leftrightarrow} CH)$$
$$CH\ believes\ CH\ controls (SU \overset{SK_2}{\Leftrightarrow} CH)$$

On message 1:

CH compares $\overset{PK_{SU}}{\longrightarrow} SU$ with the one received from the FC, and if they are same, CH **concludes that** $CH\ believes \overset{PK_{SU}}{\longrightarrow} SU$.

On message 2:

$SU\ sees\ (ID_{CH}, R_{SU}, R_{CH}, Q_1, SU \overset{SK_2}{\Leftrightarrow} CH)$ **but** $SU\ believes\ fresh\ (R_{SU})$, **therefore** $SU\ believes\ fresh\ (ID_{CH}, R_{SU}, R_{CH}, Q_1, SU \overset{SK_2}{\Leftrightarrow} CH)$.

$SU\ believes \overset{PK_{CH}}{\longrightarrow} CH$ **and** $SU\ sees\ (ID_{CH}, R_{SU}, R_{CH}, Q_1, SU \overset{SK_2}{\Leftrightarrow} CH)$, **therefore** $SU\ believes\ CH\ said\ (ID_{CH}, R_{SU}, R_{CH}, Q_1, SU \overset{SK_2}{\Leftrightarrow} CH)$. With the previous derivation **we conclude that** $SU\ believes\ CH\ believes\ (ID_{CH}, R_{SU}, R_{CH}, Q_1, SU \overset{SK_2}{\Leftrightarrow} CH)$, **and with the assumption** $SU\ believes\ CH\ controls\ (SU \overset{SK_2}{\Leftrightarrow} CH)$, **we find that** $SU\ believes\ (ID_{CH}, R_{SU}, R_{CH}, Q_1, SU \overset{SK_2}{\Leftrightarrow} CH)$, **which means** $SU\ believes\ (SU \overset{SK_2}{\Leftrightarrow} CH)$. (c)

On message 3:

$CH\ sees\ (R_{CH}, R_{SU}, ANS_1)$ and compares the received R_{CH} with the sent R_{CH}. If both are equal, CH ensures that SU has received SK_2. **Therefore**, $CH\ believes\ SU\ believes\ (SU \overset{SK_2}{\Leftrightarrow} CH)$, **and with the assumption** $CH\ believes\ CH\ controls\ (SU \overset{SK_2}{\Leftrightarrow} CH)$ **we find that** $CH\ believes\ (SU \overset{SK_2}{\Leftrightarrow} CH)$. (d)

Derivations (c) and (d) are the objectives of our proposed authentication scheme on the CH's level.

2) VERIFICATION THROUGH SCYTHER

We verified the vulnerability of the proposed authentication mechanism to potential well-known attacks such as reflection attack, man-in-the-middle attack and denial of service (DoS) attack by using the Scyther verification tool. Figures 5 and 6 prove that our protocol is safe against them. These attacks are analyzed in the following section and we show how they are eliminated through our authentication mechanism.

B. SECURITY ANALYSIS

We evaluated the proposed authentication scheme in terms of its ability to prevent the attacks described in this section. The proposed scheme is a secure scheme as long as it disallows any malicious node from accessing the network. In this section, we show the attacks that are prevented by our authentication scheme. Moreover, we show the security properties (requirements) that our two-level authentication scheme fulfills.

1) AUTHENTICATION

As mentioned above, authentication is one of the security requirements that a secure network has to fulfill. Our proposed authentication scheme ensures that a node cannot get access to network resources until it gets authenticated. Moreover, applying a two level of authentication strengthens the authentication process and reduces or even cancels the opportunity for a malicious node to cheat the FC or the CH.

2) RESOURCE AVAILABILITY AND ACCESSIBILITY

In the proposed scheme, network resources are only allocated to authenticated nodes. Nodes that are not authenticated are not allowed to access the resources; therefore, the resources are available for authenticated nodes only. This enhances network security and network performance.

3) REFLECTION ATTACK

It is an attack that targets any challenge-response authentication scheme wherein the attacker contacts a third party to get a response to the authenticating node's challenge. By our proposed authentication scheme, random numbers (nonce) are generated as a challenge to the joining node that has to send its identifier with the received nonce, as well as its own random number encrypted by its private key. The FC or the CH, whichever is the authenticator, decrypts this message and checks the random nonce number of the joining node. If they do not match, the reflection attack is detected and prevented. Therefore the reflection attack cannot be launched with our authentication scheme.

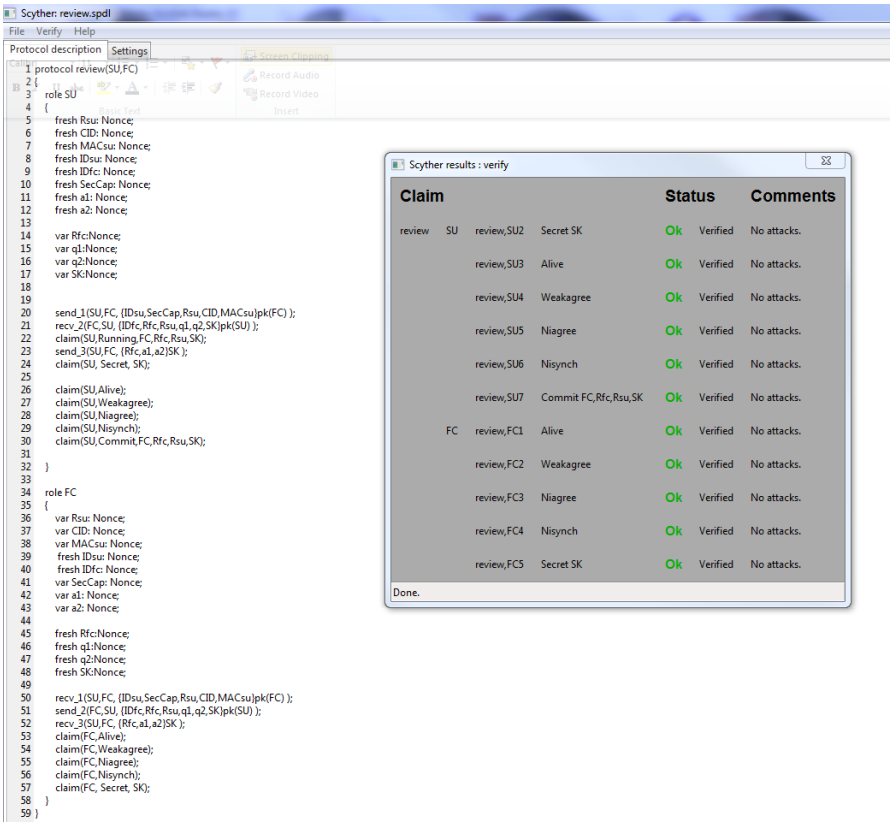

FIGURE 5. The results of executing the proposed authentication mechanism at FC level in the scyther environment.

4) MAN-IN-THE-MIDDLE ATTACK

In this attack a malicious node accesses or invades the communication between two parties. It impersonates both parties and gains access to information that the two parties were trying to send to each other. It allows a malicious actor to intercept, send, and receive data meant for someone else, or not meant to be sent at all, without either outside party knowing until the action is completed. By our proposed authentication scheme, all messages between the joining node and the authenticator (i.e. FC or CH) are encrypted by the receiver's public key or the symmetric key, which ensures that the only one that can decrypt and understand the entire message is the one that has the corresponding private key or the symmetric key. Therefore, this attack can be easily detected and avoided by our proposed authentication scheme.

5) DENIAL OF SERVICE ATTACK

A malicious node may eavesdrop on the communication between two nodes and drop the messages exchanged between the communicating nodes in order to reduce the network performance. Another example of the DoS attack is that a malicious node may inject the network with meaningless messages, which influence other nodes' performance. By our proposed authentication, the FC only accepts authentication requests from nodes that are already predefined in a manufacture list. If a node that belongs to this list launches the DoS attack, the FC will receive multiple requests from this node in order to flood the network. Therefore, the FC quickly and effectively identifies the incoming traffic as malicious. Once the flood of traffic is identified as a DoS attack, an effective response will be taken to absorb the attack, until the source is identified and blocked. This response includes releasing the assigned channels, setting its belief level value to zero and notifying the cluster heads about this node in order to prevent any node from communicating with this malicious node.

V. SCHEME PERFORMANCE EVALUATION

A. COMPLEXITY ANALYSIS

We analyze the performance overhead of our proposed Authentication algorithm. Our algorithm has two stages (at the FC or CH levels), five steps/each. In each stage, the joining node and the authenticating party exchange their first message using the other node's public key (two messages), and the other messages are sent encrypted using the symmetric key. By analyzing those messages, we find that the authenticating party (FC or CH) sends two messages, and the joining node sends three messages. As each joining node SU_i encodes three messages and decodes two messages, each joining node performs *5*O(1)* messages' encoding

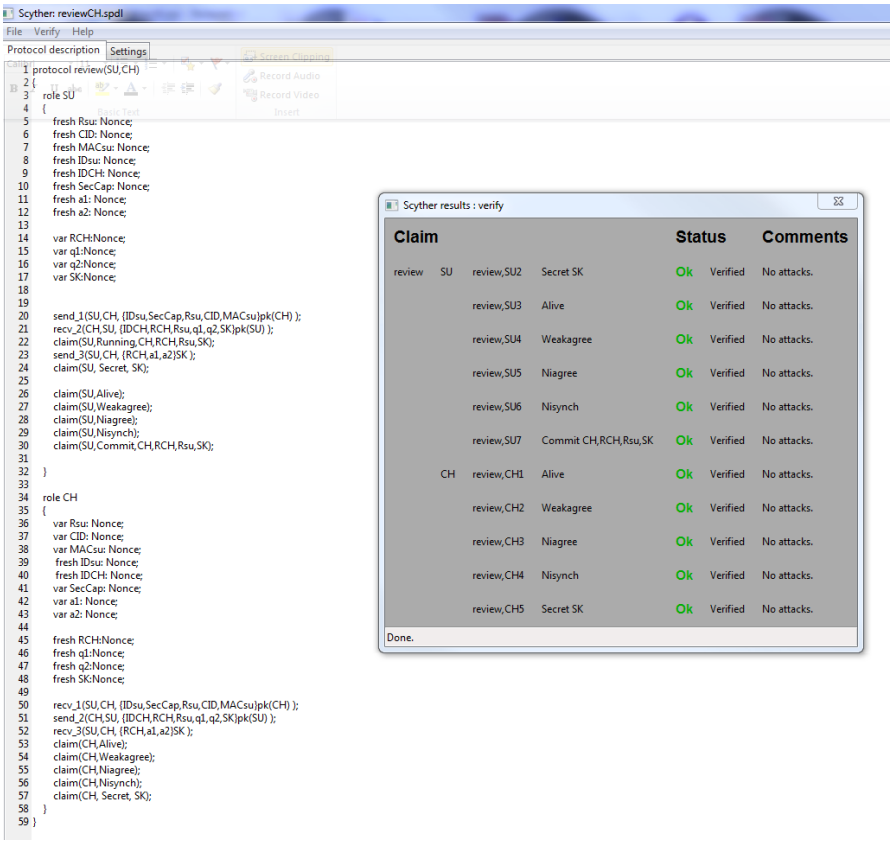

FIGURE 6. The results of executing the proposed authentication mechanism at CH level in the scyther environment.

and decoding. Thus, the computation overhead for each node is $\approx O(1)$. On the other hand, the authenticating party encodes $2*|M|$ and decodes $3*|M|$ messages, where M represents the total number of SUs. Therefore, the computation overhead at the authenticating party is $(2*|M|+3*|M|)$. If we replace M by N for complexity calculation standards, the computation overhead at the authenticating party is $\approx O(N)$. The communication overhead is calculated based on the number of messages exchanged between the joining node and the authenticating party. The number of messages is equal to that used in the computation overhead; therefore, the communication overhead at the joining SU is $\approx O(1)$ and at the authenticating party is $\approx O(N)$.

B. NUMERICAL RESULTS

In this section, we compare our proposed authentication scheme with the approaches described in [19] and [20]. This comparison is in terms of the number of cryptographic operations needed by each technique and the total authentication time. We use the benchmarks available in [24] where C++ is used to implement the cryptographic algorithms, and Microsoft Visual C++ 2005 SP1 is the compiler and the system specifications are an Intel Core 2 1.83 GHz processor under Windows Vista in 32-bit mode. We select a cryptographic algorithm for each cryptographic operation as in Table 2.

TABLE 2. Cryptographic algorithms.

Cryptographic Operation	Cryptographic Algorithm
Digital signature Generation and Verification	RSA 1024
Certificate Validation	RSA 1024
Message Encryption with Public Key	RSA 1024
Message Encryption with Symmetric Key	AES/EAX
Message Decryption with Public Key	RSA 1024
Message Decryption with Symmetric Key	AES/EAX
Hash Function	HMAC(SHA-1)

By analyzing the authentication techniques proposed in [19], in [20] and our proposed scheme and using the benchmarks in [24], we can determine how many times each cryptographic operation is executed in total, as shown in Table 3. Moreover, we use the values in Table 2 and Table 3 to compute the time needed to complete the authentication process in each approach.

To complete the authentication schemes proposed in [19 and [20], twenty-nine and thirty-nine cryptographic operations have to be executed respectively. However, in our proposed scheme only twenty-four operations are required,

TABLE 3. Cryptographic operation count.

Cryptographic Operation	Scheme		
	[19]	[20]	Proposed Approach
Certificate Validation	5	4	2
Hash Function	2	13	2
Message Encryption with Public Key	7	4	4
Message Encryption with Symmetric Key	0	6	6
Message Decryption with Public key	7	4	4
Message Decryption with Symmetric Key	0	6	6
Digital Signature Generation	4	1	0
Digital Signature Verification	4	1	0
Total	**29**	**39**	**24**

which means more than 10% less computation and calculation cost.

We next analyze the time needed to complete the authentication process, which is referred to as the authentication delay. It consists of two parts, the processing time and the transmission time. The processing time is the major part which represents the time needed to execute the cryptographic operations. The transmission time is the time needed to transmit each message between the authenticating node and the joining node. It was assumed that the transmission time was the same value in both schemes; therefore, the transmission time was omitted in the calculation of the authentication delay.

According to [24], the signature generation time is 1.48ms, the verification time using RSA 1024 is 0.07ms, the time for the message encryption with public key is 0.08ms, the time for the message decryption with public key is 1.46ms, the time for the message encryption with symmetric key is 1.8μs, the time for the message decryption with symmetric key is 1.8μs, and the hashing time using HMAC (SHA-1) is 0.509μs. The authentication time in [19] was 17.3ms and in [20] was 8.02ms. It is approximately 7.32ms in our proposed authentication scheme, which is about 57% and 9% faster in comparison to that in [19] and [20], respectively. Therefore, it is evident that our proposed scheme reduces the authentication time. Moreover, our proposed approach is less complex in comparison to that of [19] and [20]'s; since, the symmetric key cryptography is used for encrypting and decrypting most of the message exchanged. Symmetric key cryptography has less memory occupation, less memory use, and less power utilization.

VI. CONCLUSION

Cognitive radio is considered a promising technology to solve the spectrum scarcity problem. The CR nodes are more exposed to security vulnerabilities and threats because of their wireless nature. Secure communication is one of the most challenging tasks in CRNs. A CR node cannot access the spectrum unless it has been authenticated by a reliable node. In this paper, we propose a two-level secure authentication scheme in CRN wherein the authenticating node and the joining node accept a key agreement. We use the advantages of using the public key and the symmetric key cryptography to secure the messages exchanged between the communicating nodes. During the authentication process and after a symmetric key is shared between the communicating nodes, any communication will be carried out using the symmetric key cryptography.

The proposed authentication scheme, in comparison to the existing approaches, reduces the number of cryptographic operations and the authentication time needed to complete the authentication process. Moreover, the correctness of the proposed approach has been verified using the BAN logic and through the Scyther verification tool. We verified that our authentication approach is safe against many attacks.

COMPETING INTERESTS

The authors declare that they have no competing interests.

REFERENCES

[1] J. Mitola, "Cognitive radio for flexible mobile multimedia communications," in *Proc. IEEE Int. Workshop Mobile Multimedia Commun. (MoMuC)*, Nov. 1999, pp. 3–10.

[2] D. Niyato and E. Hossain, "Spectrum trading in cognitive radio networks: A market-equilibrium-based approach," *IEEE Wireless Commun.*, vol. 15, no. 6, pp. 71–80, Dec. 2008.

[3] P. Crocioni, "Is allowing trading enough? Making secondary markets in spectrum work," *Telecommun. Policy*, vol. 33, no. 8, pp. 451–468, 2009.

[4] M. Khasawneh and A. Agarwal, "A survey on security in cognitive radio networks," in *Proc. Int. Conf. Comput. Sci. Inf. Technol. (CSIT)*, 2014, pp. 64–70.

[5] Y. Akyildiz, "OFDM-based cognitive radio networks," in *Proc. Cognit. Wireless Commun. Netw.*, 2006, pp. 189–211.

[6] W. El-Hajj, H. Safa, and M. Guizani, "Survey of security issues in cognitive radio network," *J. Internet Technol.*, vol. 12, no. 2, pp. 1–18, 2011.

[7] S. Sodagari and T. C. Clancy, "An anti-jamming strategy for channel access in cognitive radio networks: Decision and game theory for security," in *Proc. LNCS*, vol. 7037. 2011, pp. 34–43.

[8] J. Zhao and G. Cao, "Robust topology control in multi-hop cognitive radio networks," in *Proc. INFOCOM*, Mar. 2012, pp. 2032–2040.

[9] M. Khasawneh, I. Kajman, R. Alkhudaidy, and A. Althubyani, "A survey on Wi-Fi protocols: WPA and WPA2," in *Proc. Int. Conf. Secur. Comput. Netw. Distrib. Syst. (SNDS)*, 2014, pp. 496–511.

[10] K. H. M. Wong, Y. Zheng, J. Cao, and S. Wang, "A dynamic user authentication scheme for wireless sensor networks," in *Proc. IEEE Int. Conf. Sensor Netw., Ubiquitous Comput., Trustworthy Comput. (SUTC)*, Jun. 2006, pp. 244–251.

[11] H.-R. Tseng, R.-W. Jan, and W. Yang, "An improved dynamic user authentication scheme for wireless sensor networks," in *Proc. GLOBECOM*, 2007, pp. 986–990.

[12] K. Han, T. Shon, and K. Kim, "Efficient mobile sensor authentication in smart home," *IEEE Trans. Consum. Electron.*, vol. 56, no. 2, pp. 591–596, May 2010.

[13] S. Zhu, S. Setia, and S. Jajodia, "LEAP: Efficient security mechanisms in large scale distributed networks," in *Proc. 10th ACM Conf. Comput. Commun. Secur. (CCS)*, 2003, pp. 62–72.

[14] P. Ning, A. Liu, and W. Du, "Mitigating DoS attacks against broadcast authentication in wireless sensor networks," *ACM Trans. Sensor Netw.*, vol. 4, no. 1, pp. 1–35, 2008.

[15] X. Tan, K. Borle, W. Du, and B. Chen, "Cryptographic link signatures for spectrum usage authentication in cognitive radio," in *Proc. 4th ACM Conf. Wireless Netw. Secur. (WiSec)*, 2011, pp. 1–12.

[16] H. S. Kim, "Location-based authentication protocol for first cognitive radio networking standard," *J. Netw. Comput. Appl.*, vol. 34, no. 4, pp. 1160–1167, 2011.
[17] S. Parvin and F. K. Hussain, "Digital signature-based secure communication in cognitive radio networks," in *Proc. Int. Conf. Broadband Wireless Comput., Commun. Appl. (BWCCA)*, 2011, pp. 230–235.
[18] S. Parvin, S. Han, B. Tian, and F. K. Hussain, "Trust-based authentication for secure communication in cognitive radio networks," in *Proc. IEEE/IFIP 8th Int. Conf. Embedded Ubiquitous Comput. (EUC)*, Dec. 2010, pp. 589–596.
[19] S. Parvin, F. K. Hussain, and O. K. Hussain, "Digital signature-based authentication framework in cognitive radio networks," in *Proc. 10th Int. Conf. Adv. Mobile Comput. Multimedia*, pp. 136–142, 2012.
[20] K. Chatterjee, A. De, and D. Gupta , "A secure and efficient authentication protocol in wireless sensor network," *Wireless Pers. Commun.*, vol. 81, no. 1, pp. 17–37, 2015.
[21] Y. Liu, P. Ning, and H. Dai, "Authenticating primary users' signals in cognitive radio networks via integrated cryptographic and wireless link signatures," in *Proc. IEEE Symp. Secur. Privacy (SP)*, May 2010, pp. 286–301.
[22] M. Burrows, M. Abadi, and R. Needham, "A logic of authentication," *ACM Trans. Comput. Syst.*, vol. 8, no. 1, pp. 18–36, 1990.
[23] C. Cremers. (2017). *Scyther User Manual*, accessed on May 16, 2017. [Online]. Available: http://profs.info.uaic.ro/~cbirjoveanu/web/Ps/Scyther/scyther-manual.pdf
[24] (2017). *Crypto++ 5.6.0 Benchmarks*, accessed on May 16, 2017. [Online]. Available: http://www.cryptopp.com/benchmarks.html

MAHMOUD KHASAWNEH received the bachelor's degree in computer engineering from the Jordan University of Science and Technology in 2010 and the M.Sc. degree from the Department of Electrical and Computer Engineering, Concordia University, in 2012, where he is currently pursuing the Ph.D. degree. During his studies at Concordia University, he has authored many journal papers, conference papers, and a book chapter. His current research is in the various aspects of cognitive radio networks including security, authentication, and routing management.

ANJALI AGARWAL (SM'03) received the B.E. degree in electronics and communication engineering from the Delhi College of Engineering, India, in 1983, the M.Sc. degree in electrical engineering from the University of Calgary, Alberta, in 1986, and the Ph.D. degree in electrical engineering from Concordia University, Montreal, in 1996. Prior to joining faculty in Concordia, she was a Lecturer with IIT Roorkee, and as a Protocol Design Engineer and a Software Engineer in industry. She is currently a Professor with the Department of Electrical and Computer Engineering, Concordia University. Her current research interests are in the various aspects of wireless networks including security and virtualization of cognitive radio networks, resource management, heterogeneous networks, and cloud networks.