Azerbaijan Journal of High Performance Computing, Vol. 2, Issue 2, 2019, pp. 141-157
https://doi.org/10.32010/26166127.2019.2.2.141.157

Authentication of Crns by Using BAN Logic

Israa N. Alsalhi, Salah A. Albermany

Kufa University, Najaf, Iraq, israan.alsalhi@student.uokufa.edu.iq, Salah.albermany@uokufa.edu.iq

*Correspondence: Israa N. Alsalhi, Kufa University, Najaf, Iraq, sraan.alsalhi@student.uokufa.edu.iq

Abstract

In broadband wireless communications, one of the main problems facing it is the limited availability of the spectrum needed to provide high-speed telecommunications services at any time and anywhere, since all radio frequencies are being reserved for different communications systems. Accordingly, a cognitive radio network (CRN) proposal was proposed to solve the problem of the limited spectrum by enhancing the overall spectrum utilization and provide an adequate spectrum for broadband wireless communications. Despite the different methods of protection used in CRNs, they may be exposed to external attacks and to provide security, we will have a high-security protocol analysis using BAN logic. BAN logic is used to analyze the protocol using to authentication; In this paper, we offer the highest protection in the contact against various attacks. We are using authentication of the ElGamal algorithm and analysis via BAN logic to show if it is achieving the authentication and secure communication to be used in CRN.

Keyword: Cognitive Radio Network, BAN Logic, Security, Spectrum Sharing, authentication, protocol, ElGamal

1. Introduction

The concept of “cognitive radio(CR)” is first presented by Mitola & Maguire, 1999. It is a new approach in wireless communications that Mitola later describe in his doctoral dissertation (Mitola, 2002). The main idea of the cognitive radio is that through the surrounding environment, it can be learned and communication in order to realize the existing spectrum in the space, reduce and limit the incidence of con-flicts (Tang & Wu, 2012).

CR is a promising environment-sensitive technique that tries to overcome the inherent non-efficient use of the spectrum is used through the application of sensing the spectrum constraints, spectrum management, spectrum sharing and mobility spec-trum (Alhakami, Mansour, Safdar, & Albermany, 2013, October).

The main tasks of CRs are sensing the spectrum, spectrum management, mobility spectrum, and spectrum sharing (Parvin, Hussain, Hussain, Han, Tian & Chang, 2012). The main objective of CR is to determine the white spaces (spectrum holes or unused spectrum) in the primary spectrum and effi-ciency in the use of this spectrum. It is used to detect without damaging the primary user. It can be detected from the transmitted signal by using only one or more meth-ods including filtering matched, detection cyclostationary feature, energy detection, collaborative detection (Spectrum sensor with a collaborative effort of CR multiple), and intervene based on the detection method including spectrum management (analy-sis plus decision making) to choose the best spectrum appropriate for users of knowledge. Mobility spectrum allocation is the best possible range of movement during the process of the user's knowledge. Finally, spectrum sharing is a way to schedule just in the use of the spectrum. Today, more than 5000 million devices are in use; it is expected that it will be more than 10 billion by 2017 and about 100 bil-lion by the year 2025. This number includes smartphones, tablets, and laptops to mobile networks. Radios cognitive future availability of new technology with nano-technology and numerous advantages and features include smart antennas, the new device included) with the definition of radio spectrum sensing program, measurement of the spectrum, monitoring of middle income, guidance, self-regulating, and control mechanisms to adapt, learning, identify policies and monitoring. It requires the de-velopment and introduction of new technology and measuring appropriate security policies. So security at every step of cognitive wireless networks is a difficult tasks (Reddy, 2013, June).

However, as is the case with many novel technologies, Studies and preliminary research did not focus on the security areas of CR. Security is usually "pulled on" after the truth by adding some arrangement of linking authentication and encryption. This typically works well for data reflecting a wireless network, but superfluous for the things essential to run Wireless link itself. We need to look at menaces. We de-fine three classes of attacks: Sensory handling attacks against policy radios, self-propagating conduct leading CR viruses, and faith manipulation attacks against learn-ing radios. All kinds of attacks dealing with the behavior of a CR, so that works either sub-optimally or until maliciously (Clancy & Goergen, 2008, May).

Despite the presence of a trusted entity in the central CRNs caring for key management, documentation, and so on, the challenge of providing security still a critical challenge in the decentralized architecture through not found such an entity (Mishra, Mathew & Lau, 2016). Compared to the centralized, from the infor-mation contained in a central dedicated CRNs, are more prone to nonstandard behav-ior, such as fraud, tapping, Ministry of Foreign Affairs and replay attacks. You can target these weaknesses through the inherent weaknesses in the safe design of MAC protocols that are used to provide the vital authentication mechanisms and secure connection. Therefore, we should make every effort to ensure the security aspects strong enough, simpler authentication, authorization, integrity, confidentiality and non-repudiation.

Used on a large scale and a large number of security technologies, on a symmet-rical basis (such as DES) and asymmetric encryption (such as RSA) We can achieve security in networks (Stallings, 2017).

In this paper, we will use the ElGamal encryption, even though the certification authority (CA) and digital certificate (DC) technologies play an important role in providing security against any malicious users. Digital signatures (DS) can provide more safety to ensure integrity and non-repudiation. It is very important to make sure of any design that meets the security needs of the protocol and analyzes the require-ments of security fully before being released. We will use one of the methods of anal-ysis and verification of security protocols. It is BAN logic (Burrows, Abadi & Needham, 1989). In this paper, a novel MAC protocol for secure networks Cognitive radio (SMC) have been proposed and analyzed using formal logic BAN (Syverson, P., & Cervesato, I., 2000, September). A logic that is applied to the study of the suggested protocol in order to ensure that the proposed protocol is strict enough in terms of the main security aspects.

2. Related Work

MAC protocol plays an important role in the spectrum (Bhandari & Moh, 2015). Channel joint control is the most challenging in CR networks are a bottle-neck, and any threat is considered a threat to the network (Idoudi, Daimi & Saed, 2014, July). So we have to provide security to ensure the integrity of the network security and there are many studies in this area. For example: Elkashlan, Wang, Duong, Karagiannidis & Nallanathan, (2014) proposed physical-layer security development in cognitive multiantenna eavesdropping chan-nels. In passive wiretap tries to evaluate the secrecy performance, we adopt the secrecy cutout probability as a measure of beneficial performance where it is considered the cognitive wiretap channel and as a proposed multiple antennas to secure the broadcast-ing at the physical layer, where the eavesdropper hears the transmission from the sec-ondary transmitter to the secondary receiver (Thakre & Dixit, 2014). This is to discover the threats from the wireless communication and sense the null spectrum band by Energy sensing method and to work in two ways of threats like (jamming attack and primary user emulation attack). These two are the major threats of the CRN wireless communication environment (Zhang, Lu, Cheng, Mark, & Shen, 2013).

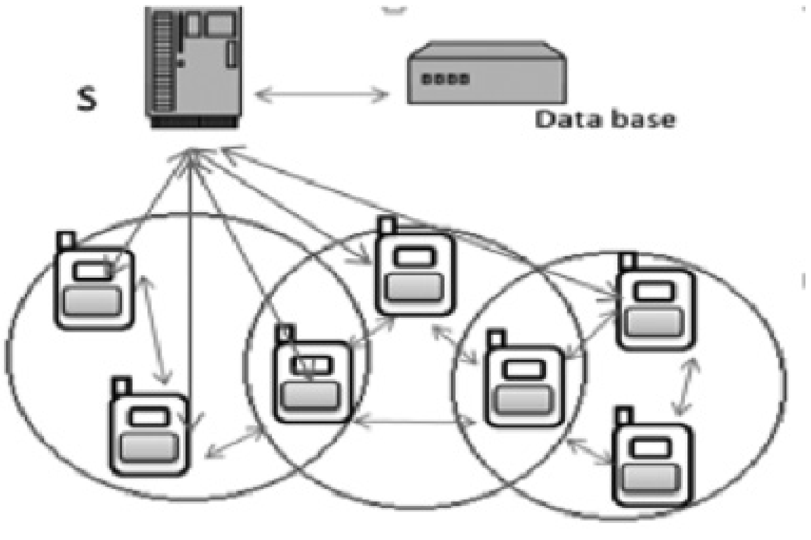


Fig. 1: Communication in CRNs

Looked at access to the cooperative spectrum for CRNs, which is a goal to enhancement the secure transmission of the primary user via cooperating the second user that would be invented by assured transmission opportunities (Tang, L., & Wu, J., 2012). It gives the first details about the analysis of the security problems encoun-tered by the CRN and enters the key issues about CRN. Then, according to the non-consistencies between the CRN and the wireless network current, it analyzes and dis-cusses the access spectrum and artificial intelligence security dynamic. Lastly, it con-cludes that the security difficulties of the cross-layer layout.

3. System Model.

In this system, the user authentication through the server where it is generating public key from the server in cooperation with users has to be known to the parties and in return, are generating a private key that each party is only known to the Party concerned. The authentication scheme can be illustrated as follows:

3.1. The Proposed User Authentication Scheme

In this section, a user authentication scheme based on ElGamal encryption and analy-sis via BAN Logic is discussed. The proposed scheme is divided into three phases: Setup phase, User authentication phase, and encryption phase. In the setup phase, CA produces system parameters and distributed them to users. In the second phase, users finish their identities authentication with the assistance of their public/ private keys and also the public key of CA. In the user encryption phase, users obtain their pri-vate/public key pairs by registering with CA.

The Setup Phase

Key Generation

With ElGamal, just the receiver needs to generate a key previously and publish it.

The following steps will be taken by Node B to generate his key pair:

- Prime and group generation

The server generates a large prime q and the generator (a) of a multiplicative

Private Key selection

Node B selects an integer (XB) less than (q–1). We will deal with him here as a private exponent.

- Public key assembling

From this we can calculate the public key portion (a^{XB} mod q). The public key of Bob in the ElGamal cryptosystem is the triplet (a; q; YB) and his private key will be (XB).

- Public key publishing

The public key now needs to be published using some present with the key server or other means; for this reason, Node A can get hold of it.

- Encryption Procedure

To encrypt a message M to Node B, Alice needs to get his public key triplet (a; q; YB) from a key server. For the encryption of the plaintext message M, node A performs the following steps:

- Obtain the public key

As explained above, Node A has to obtain the public key part (a; q; YB) from Node B.

- Present M for encoding

Write M as an integer (0 < M < q - 1).

- Select random exponent

Node A will choose a random exponent (k1) that lies on the second party's private exponent in the Diffie-Hellman key exchange. The randomness is an essential factor as the likelihood to estimate the k gives a sensible amount of the Information necessary in order for the attacker to receive the decrypted message.

- Compute key

To transfer the random exponent k1 to Node B, Node A computes ((YB)k1 mod q) and merge it with the ciphertext that is sent to Node B.

Encrypt the plaintext

Node A encrypts the message M to the ciphertext C.

The User Authentication Phase

MSG 1: A → S: A, B;

MSG 2: S →B: {NB, # (a, q), KS} KS-1;

MSG 3: B→S: {NA, YB, KS, A} KB;

MSG 4: S →A: {NA, #(M) , KS, B} KS-1 ;

MSG 5: A →B: {NA, C1, C2, KA} KA;

MSG 6: B →A: {K, M', KA} KB;

The Encryption Phase

Algorithm (1): Authentication using (ElGamal algorithm)

Input: Request from CHs.

Output: Authenticate or not.

1 - CHs sends a request to server S for node A wants to communicate with node B.

2 - Server selects two random numbers {a, q}, where a < q

a: Generator number

q: Random prime number

The server sends {a, q, request from CHs} to node B

3 - $B = \begin{cases} \text{Selects } (X_B) < (q - 1)\text{: as secret key} \\ \text{Computes } Y_B = a^{XB} \bmod q\text{: sends to the server} \end{cases}$

4 - Server= $\begin{cases} \text{Public key } \{a, q, Y_B\} \text{ and sends it to node A v} \\ \text{Sends a plain text as an integer M, } 0 < M < q - 1 \end{cases}$

5 - $$A=\begin{cases}\text{Select integer number (k1), } 0 < k1 < q-1\\ K=(Y_B)^{k1} \bmod q\\ \text{Cipher text } (C_1, C_2), C_1 = a^{k1} \bmod q, \quad C_2 = M\,K \bmod q\\ \text{Sends } \{C_1, C_2, YA, M\} \text{ to node B}\end{cases}$$

6 - $$B=\begin{cases}K2 = C_1^{XB} \bmod q\\ M' = C_2\,K_2^{-1} \bmod q\\ C'_1 = a^{k1} \bmod q\\ C'_2 = M'\,K \bmod q\\ \text{A is authenticated and sends } \{C'_1, C'_2\} \text{ to A, if } M' = M\\ \text{A is not authenticated} \qquad\qquad \text{Otherwise}\end{cases}$$

7 - CHs sent request to the server for node B wants to communicate with node C.

8 - $$\text{Server}=\begin{cases}\text{Selects two random number (a1,q1)}\\ \text{Server sends } \{a1, q1, \text{request from } CH_S\} \text{ to node C}\end{cases}$$

Where a1: Generator number and q1: Random prime number.

9 - $$C=\begin{cases}\text{Selects an integer (Xc)} < q1-1 \text{ ,as a secret key}\\ YC = a^{XC} \bmod q, \text{ sends the result to the server}\end{cases}$$

10 - $$S=\begin{cases}\text{Public key } \{a1, q1, YC\} \text{ and sents it to node B}\\ \text{Sends a plain text as an integer M, where } 0 < M < q1-1\end{cases}$$

11 - $$B=\begin{cases}\text{Selects an integer number (k1), } 0<k1<q1-1\\ K = (YC)^{k1} \bmod q1\\ \text{Cipher text } (C_3 \text{ and } C_4), C_3=a^{k1} \bmod q1 , C_4=M1K \bmod q1\\ \text{Sends } \{C_3 , C_4 , YC , M\} \text{to node C}\end{cases}$$

12 - $$C=\begin{cases}K_2= C_3^{XC} \bmod q1\\ M'_1=C_4K_2^{-1} \bmod q1\\ C'_3=a^{k1} \bmod q1\\ C'_4=M'1K\text{mod } q1\\ \text{B is authenticated and send } \{C'3, C'4\} \text{to B , If } M'1 = M\\ \text{B is not authenticated} \qquad\qquad \text{otherwise}\end{cases}$$

The original messages of authentication phase are representing as follow:

MSG 1: CHs → S: A, B from CHs

MSG 2: S → B: {NB, # (a, q), KS} KS-1 from S

MSG 3: B → S: {NA, YB, KS, A} KB from B

MSG 4: S → A: {NA, # (M), KS, B} KS-1 from S

MSG 5: A → B: {NA, C1, C2, KA} KA from A

MSG 6: B → A: {K, M', KA} KB from B

MSG 7: CHs → S: B, C from CHs

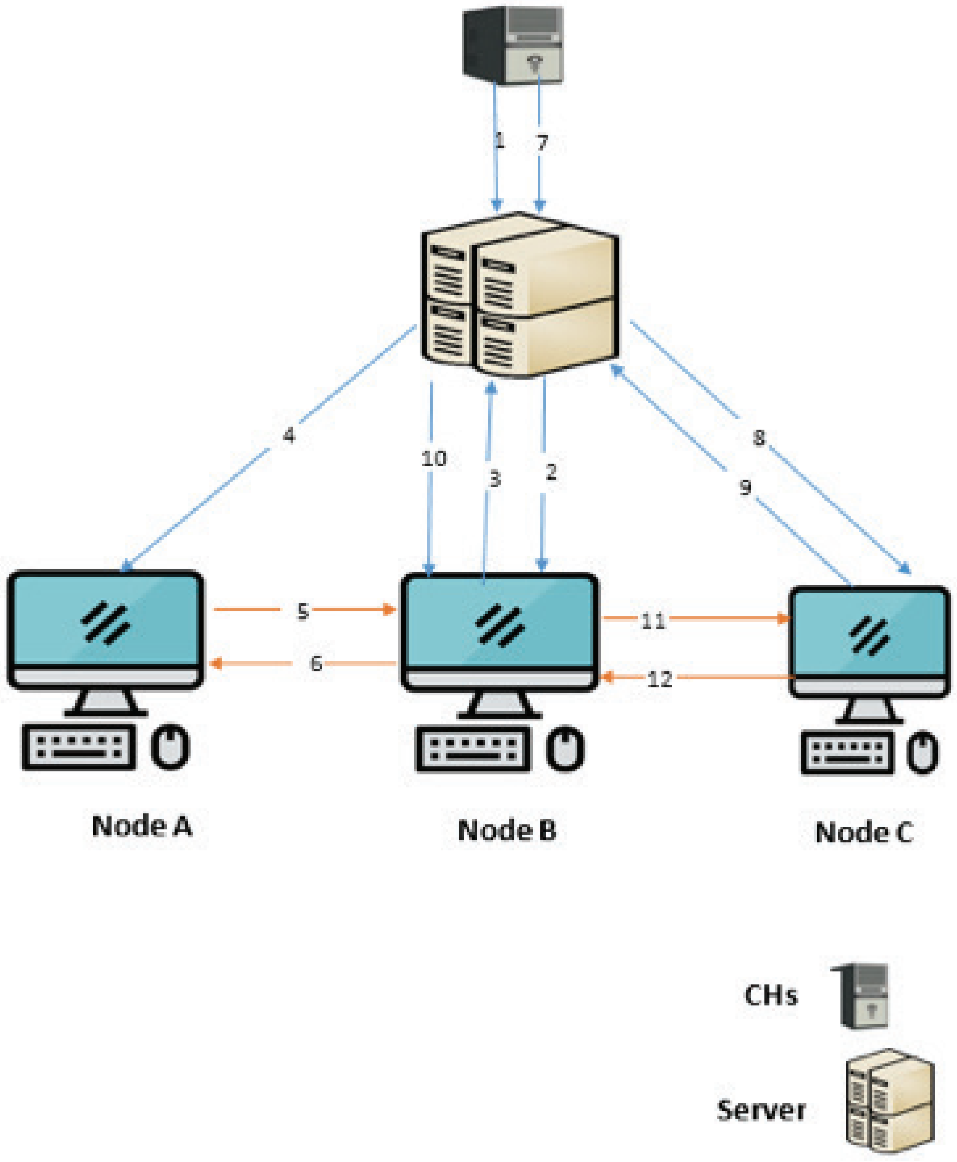


Fig. 2: . Authentication using (ElGamal algorithm)

MSG 8: S → C: {NC, # (a1, q1), KS} KS-1 from S

MSG 9: C → S: {NB, Yc, KS, B} KC from C

MSG 10: S → B: {NB, # (M), KS, C} KS-1 from S

MSG 11: B → C: {NB, C1, C2, KB} KB from B

MSG 12: C → B: {Nc, K, M', Kc} KC from C.

4. Security and Performance Analysis

4.1. Security analysis by BAN logic

Burrows-Abadi-Needham(BAN) Logic is One of the methods for analyzing authentication protocols; It is a logic for reasoning about authentication protocol in terms of belief statements (Abadi, M., & Tuttle, M. R., 1991, August, Wessels, J., & BV, C. F., 2001). It is using different symbols in the cryptographic scheme as follows:

① P believes X: P |≡X;

② p receive X: p ⊳X;

③ P send X: P|∼X;

④ P controls X: P | ⇒ X;

⑤ X is fresh: #(X);

⑥ P and Q shared by the key K: $p \overset{k}{\leftrightarrow} Q$;

⑦ ciphertext of X encrypted by the key K: {X}K;

Rule of BAN logic:

Message meaning: This rule allow the identity of the sender of an encrypted message to be deduced from the encryption key used.

$$\frac{p \mid\equiv\ Q \overset{k}{\leftrightarrow} p, p\ \rhd \{x\}_k}{p \mid\equiv Q| \sim x} \tag{1}$$

The key K shares Q and P. So, if P receives a message encrypted by K, it must come from Q (P ignores its messages).

Nonce-verification:-This rule allow belief from freshly uttered message to be derived

$$\frac{p \mid\equiv \#(x), p \mid\equiv Q| \sim x}{p \mid\equiv Q| \equiv x} \tag{2}$$

Jurisdiction rule: This rule allows belief based on jurisdiction to be derived.

$$\frac{p \mid\equiv\ Q \overset{k}{\Rightarrow} x, p \mid\equiv Q| \equiv x}{p \mid\equiv x} \tag{3}$$

The idealized protocol as follows:

Message (1) and message (7) will be deleted because it does not contain an encrypted message. The rest of the messages will be represented as follow:

MSG 2: B ⊳{NB, # (a, q), $\overset{KS}{\rightarrow}$S} KS-1

MSG 3: S ⊳{NA, YB, $\overset{KS}{\rightarrow}$S} KB

MSG 4: A ⊳{NA, # (M), $\overset{KS}{\rightarrow}$S} KS-1

MSG 5: B ⊳ {NA, C1, C2, $\overset{KA}{\rightarrow}$A} KA

MSG 6: A ⊳ {K, M', $\overset{KA}{\rightarrow}$A} KB

MSG 8: C⊳ {NC, # (a1, q1), $\overset{KS}{\rightarrow}$ S} KS-1

MSG 9: S $\rhd$\{NB, Yc, $\xrightarrow{KS}$S\} KC

MSG 10: B $\rhd$\{NB, # (M), $\xrightarrow{KS}$S\} KS-1

MSG 11: C $\rhd$\{NB, C1, C2, $\xrightarrow{KB}$B\} KB

MSG 12: B $\rhd$\{K, M', $\xrightarrow{KB}$B\} KC

State assumption about the original message

$S| \# NB$ (1.1)

$S| \equiv \#a$ (1.2)

$S| \equiv \#q$ (1.3)

$S| \equiv \# NA$ (1.4)

$S| \equiv \#M$ (1.5)

$B| \equiv \# NA$ (1.6)

$A| \equiv \# NA$ (1.7)

$S| \equiv \xrightarrow{KB} B$ (1.8)

$S |\equiv B| \Rightarrow \xrightarrow{KS} S$ (1.9)

$B |\equiv A| \Rightarrow \xrightarrow{K_A} A$ (1.10)

$C| \equiv \xrightarrow{K_S} S$ (1.11)

$C | \equiv S \Rightarrow \xrightarrow{KS} S$ (1.12)

$B | \equiv S| \Rightarrow \xrightarrow{KS} S$ (1.13)

$S| \equiv \xrightarrow{KC} C$ (1.14)

$B| \equiv \xrightarrow{K_C} C$ (1.15)

$S| \equiv \xrightarrow{K_S} S$ (1.16)

$B| \equiv \xrightarrow{KS} S$ (1.17)

$B| \equiv \xrightarrow{K_B} B$ (1.18)

$A| \equiv \xrightarrow{KS} S$ (1.19)

$A| \equiv \xrightarrow{KA} A$ (1.20)

$B| \equiv \xrightarrow{KA} A$ (1.21)

$A| \equiv \xrightarrow{K_B} B$ (1.22)

$B | \equiv S| \Rightarrow \xrightarrow{KS} S$ (1.23)

$A |\equiv S| \Rightarrow \xrightarrow{KS} S$ (1.24)

$A |\equiv B| \Rightarrow \xrightarrow{K_A} A$ (1.24)

$C| \equiv \#(NC)$ (1.26)

$B| \equiv C \Rightarrow \xrightarrow{K_B} B$ (1.27)

$C |\equiv B| \Rightarrow \xrightarrow{K_B} B$ (1.28)

$C | \equiv \#(NB)$ (1.29)

$S |\equiv C| \Rightarrow \xrightarrow{KS} S$ (1.30)

Apply rule:

MSG 2: B $\rhd$ \{NB, # (a, q), $\xrightarrow{KS}$S\} KS-1from S

By applying equation (1) to message (2), produces the following:

$$\frac{B|\equiv \xrightarrow{K_S} S, B \rhd \{NB, \#(a, q), \xrightarrow{KS} B\} KS-1}{B |\equiv S| \sim \xrightarrow{K_S} S} \qquad (1,2)$$

By applying equation (2) to message (2), produces the following:

$$\frac{B |\equiv \#(NA), B |\equiv S| \sim \xrightarrow{K_S} S}{B |\equiv S| \equiv \xrightarrow{K_S} S} \qquad (2.2)$$

By applying equation (3) to message (2), produces the following:

$$\frac{\mathrm{B} \mid\equiv \mathrm{S} \Rightarrow \xrightarrow{KS} \mathrm{S}, \mathrm{p} \mid\equiv \mathrm{Q} \mid\equiv \mathrm{x}}{\mathrm{B} \mid\equiv \xrightarrow{K_S} \mathrm{S}} \tag{3.2}$$

The result from equation (2.2) and (3.2) are: $\mathrm{B} \mid\equiv \mathrm{S} \mid \equiv \xrightarrow{K_S} \mathrm{S}$ (2.2.1)

$$\mathrm{B} \mid \equiv \xrightarrow{K_S} \mathrm{S} \tag{3.2.1}$$

MSG 3: S ⊳ {NA, YB, $\xrightarrow{KS}$S} KB

By applying equation (1) to message (3), produces the following:

$$\frac{\mathrm{S} \mid\equiv \xrightarrow{KB} \mathrm{B}, \left\{ \mathrm{NA}, \mathrm{YB}, \xrightarrow{KS} \mathrm{S} \right\} \mathrm{KB}}{\mathrm{S} \mid\equiv \mathrm{B} \mid\sim \xrightarrow{KS} \mathrm{S}} \tag{1.3}$$

By applying equation (2) to message (3), produces the following:

$$\frac{\mathrm{p} \mid\equiv \#(Nb), \mathrm{S} \mid\equiv \mathrm{B} \mid\sim \xrightarrow{KS} \mathrm{S}}{\mathrm{S} \mid\equiv \mathrm{B} \mid\equiv \xrightarrow{K_S} \mathrm{S}} \tag{2.3}$$

By applying equation (3) to message (3), produces the following:

$$\frac{S \mid\equiv \mathrm{B} \mid\Rightarrow \xrightarrow{KS} \mathrm{S}, \mathrm{S} \mid\equiv \mathrm{B} \mid\equiv \xrightarrow{KS} \mathrm{S}}{\mathrm{S} \mid\equiv \xrightarrow{K_S} \mathrm{S}} \tag{3.3}$$

The result from equation (2.3) and (3.3) are: $\mathrm{S} \mid\equiv \mathrm{B} \mid \equiv \xrightarrow{KS} \mathrm{S}$ (2.3.1)

$$\mathrm{S} \mid \equiv \xrightarrow{\mathrm{K_S}} \mathrm{S} \tag{3.3.1}$$

MSG 4: A ⊳ {NA, # (M) , $\xrightarrow{KS}$S } KS-1

By applying equation (1) to message (4), produces the following:

$$\frac{\mathrm{A} \mid\equiv \xrightarrow{kS} \mathrm{S}, \mathrm{A} \rhd \{ \mathrm{NA}, \#(\mathrm{M}), \xrightarrow{KS} \mathrm{S} \} \mathrm{KS}-1}{\mathrm{A} \mid\equiv \mathrm{S} \mid\sim \xrightarrow{KS} \mathrm{S}} \tag{1.4}$$

By applying equation (2) to message (4), produces the following:

$$\frac{\mathrm{A} \mid\equiv \#(\mathrm{NA}), \mathrm{A} \mid\equiv \mathrm{S} \mid \sim \xrightarrow{KS} \mathrm{S}}{\mathrm{A} \mid\equiv \mathrm{S} \mid\equiv \xrightarrow{KS} \mathrm{S}} \tag{2.4}$$

By applying equation (3) to message (4), produces the following:

$$\frac{A \mid\equiv \mathrm{S} \mid\Rightarrow \xrightarrow{KS} \mathrm{S}, \mathrm{p} \mid\equiv \mathrm{Q} \mid\equiv \mathrm{x}}{\mathrm{A} \mid\equiv \xrightarrow{KS} \mathrm{S}} \tag{3.4}$$

The result from equation (2.4) and (3.4) are: $\mathrm{A} \mid\equiv \mathrm{S} \mid \equiv \xrightarrow{KS} \mathrm{S}$ (2.4.1)

$$\mathrm{A} \mid \equiv \xrightarrow{K_S} \mathrm{S} \tag{3.4.1}$$

MSG 5: B ⊳ {NA, C1, C2, $\xrightarrow{KA}$A} KA

By applying equation (1) to message (5), produces the following:

$$\frac{\mathrm{B} \mid\equiv \xrightarrow{kA} \mathrm{A}, \mathrm{B} \rhd \{ \mathrm{NA}, \mathrm{C1}, \mathrm{C2}, \xrightarrow{K_A} \mathrm{A} \} \mathrm{KA}}{\mathrm{B} \mid\equiv \mathrm{A} \mid\sim \xrightarrow{K_A} \mathrm{A}} \tag{1.5}$$

By applying equation (2) to message (5), produces the following:

$$\frac{\mathrm{B}\ |{\equiv}\#(\mathrm{NA}),\mathrm{B}\ |{\equiv}\mathrm{A}|{\sim}\xrightarrow{K_A}\mathrm{A}}{\mathrm{B}\ |{\equiv}\mathrm{A}|{\equiv}\xrightarrow{K_A}\mathrm{A}} \tag{2.5}$$

By applying equation (3) to message (5), produces the following:

$$\frac{\mathrm{B}\ |{\equiv}\mathrm{A}|{\Rightarrow}\xrightarrow{K_A}\mathrm{A}\ ,\mathrm{B}\ |{\equiv}\mathrm{A}|{\equiv}\xrightarrow{K_A}\mathrm{A}}{\mathrm{B}\ |{\equiv}\xrightarrow{K_A}\mathrm{A}} \tag{3.5}$$

The result from equation (2.5) and (3.5) are: $\mathrm{B}\ |{\equiv}\ \mathrm{A}|\ {\equiv}\overset{K_A}{\rightarrow}\mathrm{A}$ (2.5.1)

$$\mathrm{B}\ |\ {\equiv}\overset{K_A}{\rightarrow}\mathrm{A} \tag{3.5.1}$$

MSG 6: A ⊳ {K, M', $\overset{K_A}{\rightarrow} A$ } KB

By applying equation (1) to message (6), produces the following:

$$\frac{\mathrm{A}|{\equiv}\xrightarrow{K_B}\mathrm{B},\mathrm{A}\rhd\left\{\mathrm{K},\mathrm{M}',\xrightarrow{K_A}A\right\}\mathrm{KB}}{\mathrm{A}\ |{\equiv}\mathrm{B}|{\sim}\xrightarrow{K_A}A} \tag{1.6}$$

By applying equation (2) to message (6), produces the following:

$$\frac{\mathrm{A}\ |{\equiv}\#(\mathrm{NA}),\mathrm{A}\ |{\equiv}\mathrm{B}|{\sim}\xrightarrow{K_A}A}{\mathrm{A}\ |{\equiv}\mathrm{B}|{\equiv}\xrightarrow{K_A}A} \tag{2.6}$$

By applying equation (3) to message (6), produces the following:

$$\frac{\mathrm{A}\ |{\equiv}\mathrm{B}|{\Rightarrow}\xrightarrow{K_A}\mathrm{A}\ ,\mathrm{A}\ |{\equiv}\mathrm{B}|{\equiv}\xrightarrow{K_A}A}{\mathrm{A}\ |{\equiv}\overset{A}{\rightarrow}\mathrm{A}} \tag{3.6}$$

The result from equation (2.6) and (3.6) are:

$$\mathrm{A}\ |{\equiv}\ \mathrm{B}|\ {\equiv}\overset{K_A}{\rightarrow}A \tag{2.6.1}$$

$$\mathrm{A}\ |\ {\equiv}\overset{A}{\rightarrow}\mathrm{A} \tag{3.6.1}$$

MSG 8: C ⊳ { NC , # (a1 , q1), KS } KS-1

By applying equation (1) to message (8), produces the following:

$$\frac{\mathrm{C}|{\equiv}\xrightarrow{K_S}\mathrm{S}\ ,\mathrm{C}\rhd\{\ \mathrm{NC}\ ,\#\ (\ \mathrm{a1}\ ,\mathrm{q1}\ ),\mathrm{KS}\ \}\ \mathrm{KS}^{-1}}{C\ |{\equiv}\mathrm{S}|{\sim}\xrightarrow{K_S}\mathrm{S}} \tag{1.8}$$

By applying equation (2) to message (8), produces the following:

$$\frac{\mathrm{C}|{\equiv}\#(\mathrm{NC}),\mathrm{C}\ |{\equiv}\mathrm{S}|{\sim}\xrightarrow{K_S}\mathrm{S}}{\mathrm{C}|{\equiv}\mathrm{S}|{\equiv}\xrightarrow{K_S}\mathrm{S}} \tag{2.8}$$

By applying equation (3) to message (8), produces the following:

$$\frac{\mathrm{C}\ |{\equiv}\ \mathrm{S}\Rightarrow\xrightarrow{KS}\mathrm{S}\ ,\mathrm{C}|{\equiv}\mathrm{S}|{\equiv}\xrightarrow{K_S}\mathrm{S}}{\mathrm{C}\ |{\equiv}\xrightarrow{K_S}\mathrm{S}} \tag{3.8}$$

The result from equation (2.8) and (3.8) are: $\mathrm{C}\ |{\equiv}\ \mathrm{S}|\ {\equiv}\overset{K_S}{\rightarrow}\mathrm{S}$ (2.8.1)

$$\mathrm{C}|\ {\equiv}\overset{K_S}{\rightarrow}\mathrm{S} \tag{3.8.1}$$

MSG 9: $\mathrm{S}\ \rhd\ \{\ \mathrm{NB}\ ,\mathrm{YC}\ ,\overset{KS}{\rightarrow}\mathrm{S}\}$ KC

By applying equation (1) to message (9), produces the following:

$$\frac{\mathrm{S}|\equiv\xrightarrow{KC}\mathrm{C}\ ,\mathrm{S}\rhd\{\ \mathrm{NB}\ ,\mathrm{YC}\ ,\xrightarrow{KS}\mathrm{S}\}\ \mathrm{KC}}{\mathrm{S}\ |\equiv\mathrm{C}|\sim\xrightarrow{KS}\mathrm{S}} \tag{1.9}$$

By applying equation (2) to message (9), produces the following:

$$\frac{\mathrm{S}\ |\equiv\#(\mathrm{NB}),\mathrm{S}\ |\equiv\mathrm{C}|\sim\xrightarrow{KS}\mathrm{S}}{\mathrm{S}\ |\equiv\mathrm{C}|\equiv\xrightarrow{K_S}\mathrm{S}} \tag{2.9}$$

By applying equation (3) to message (9), produces the following:

$$\frac{S\ |\equiv\mathrm{C}|\Rightarrow\xrightarrow{KS}\mathrm{S},\mathrm{S}\ |\equiv\mathrm{C}|\equiv\xrightarrow{KS}\mathrm{S}}{\mathrm{S}\ |\equiv\xrightarrow{K_S}\mathrm{S}} \tag{3.9}$$

The result from equation (2.9) and (3.9) are: $\mathrm{S}\ |\equiv\ \mathrm{C}|\ \equiv\xrightarrow{KS}\mathrm{S}$ (2.9.1)

$$\mathrm{S}\ |\ \equiv\xrightarrow{K_S}\mathrm{S} \tag{3.9.1}$$

MSG 10: S → $\mathrm{B}\ \rhd\ \{\ \mathrm{NB},\#(\ \mathrm{M}\ ),\xrightarrow{KS} S\ \}$ KS-1

By applying equation (1) to message (10), produces the following:

$$R1=\frac{\mathrm{B}|\equiv\xrightarrow{kS}\mathrm{S},\mathrm{B}\rhd\{\ \mathrm{NB},\#(\ \mathrm{M}\ )\ ,\xrightarrow{KS}\mathrm{S}\ \}\ \mathrm{KS}-1}{\mathrm{B}\ |\equiv\mathrm{S}|\sim\xrightarrow{KS}\mathrm{S}} \tag{1.10}$$

By applying equation (2) to message (10), produces the following:

$$R2=\frac{\mathrm{B}\ |\equiv\#(\mathrm{NB}),\mathrm{B}\ |\equiv\mathrm{S}|\ \sim\xrightarrow{KS}\mathrm{S}}{\mathrm{B}\ |\equiv\mathrm{S}|\equiv\ \xrightarrow{KS}\mathrm{S}} \tag{2.10}$$

By applying equation (3) to message (10), produces the following:

$$R3=\frac{B\ |\equiv\mathrm{S}|\Rightarrow\xrightarrow{KS}\mathrm{S},\mathrm{B}\ |\equiv\mathrm{S}|\equiv\ \xrightarrow{KS}\mathrm{S}}{\mathrm{B}\ |\equiv\ \xrightarrow{KS}\mathrm{S}} \tag{3.10}$$

The result from equation (2.10) and (3.10) is: $\mathrm{B}\ |\equiv\ \mathrm{S}|\ \equiv\ \xrightarrow{KS}\mathrm{S}$ (2.10.1)

$$\mathrm{B}\ |\ \equiv\xrightarrow{K_S}\mathrm{S} \tag{3.10.1}$$

MSG 11: B → $\mathrm{C}\ \rhd\ \{\ \mathrm{NB}\ ,\mathrm{C1},\mathrm{C2},\xrightarrow{K_B}\mathrm{B}\}$ KB

By applying equation (1) to message (11), produces the following:

$$\frac{\mathrm{B}|\equiv\xrightarrow{kB}\mathrm{B}\ ,\mathrm{C}\rhd\{\ \mathrm{NB}\ ,\mathrm{C1},\mathrm{C2},\xrightarrow{K_B}\mathrm{B}\}\ \mathrm{KB}}{\mathrm{C}\ |\equiv\mathrm{B}|\sim\ \xrightarrow{K_B}\mathrm{B}} \tag{1.11}$$

By applying equation (2) to message (11), produces the following:

$$\frac{\mathrm{C}\ |\equiv\#(\mathrm{NB}),\mathrm{C}\ |\equiv\mathrm{B}|\sim\ \xrightarrow{K_B}\mathrm{B}}{\mathrm{C}\ |\equiv\mathrm{B}|\equiv\ \xrightarrow{K_B}\mathrm{B}} \tag{2.11}$$

By applying equation (3) to message (11), produces the following:

$$\frac{\mathrm{C}\ |\equiv\mathrm{B}|\Rightarrow\ \xrightarrow{K_B}\mathrm{B},C|\equiv\mathrm{B}|\equiv\ \xrightarrow{K_B}\mathrm{B}}{\mathrm{C}|\equiv\xrightarrow{K_B}\mathrm{B}} \tag{3.11}$$

The result from equation (2.11) and (3.11) is: $\mathrm{C}\ |\equiv\ \mathrm{B}|\ \equiv\ \xrightarrow{K_B}\mathrm{B}$ (2.11.1)

$$\mathrm{C}|\ \equiv\xrightarrow{K_B}\mathrm{B} \tag{3.11.1}$$

$$\mathrm{C}| \equiv \xrightarrow{K_B} \mathrm{B} \qquad (3.11.1)$$

MSG 12: C→ $\mathrm{B} \vartriangleright \left\{ \mathrm{K}, \mathrm{M}', \xrightarrow{K_B} B \right\}$} KC

By applying equation (1) to message (12), produces the following:

$$\frac{\mathrm{B}|\equiv \xrightarrow{K_C} \mathrm{C,B} \vartriangleright \left\{ \mathrm{K,M}', \xrightarrow{K_B} B \right\} \mathrm{KC}}{\mathrm{B}\ |\equiv \mathrm{C}|\sim \xrightarrow{K_B} B} \qquad (1.12)$$

By applying equation (2) to message (12), produces the following:

$$\frac{\mathrm{B}\ |\equiv \#(\mathrm{NB}),\mathrm{B}\ |\equiv \mathrm{C}|\sim \xrightarrow{K_B} B}{\mathrm{B}\ |\equiv \mathrm{C}|\equiv \xrightarrow{K_B} B} \qquad (2.12.)$$

By applying equation (3) to message (12), produces the following:

$$\frac{\mathrm{B}\ |\equiv \mathrm{C}|\Longrightarrow \xrightarrow{K_B} \mathrm{B}\ ,\mathrm{B}\ |\equiv \mathrm{C}|\equiv \xrightarrow{K_B} B}{\mathrm{B}\ |\equiv \overset{B}{\rightarrow} \mathrm{B}} \qquad (3.12)$$

The result from equation (2.12) and (3.12) is $\mathrm{B} \mid \equiv \mathrm{C}| \equiv \xrightarrow{K_B} B$ (2.12.1)

$$\mathrm{B} \mid \equiv \overset{B}{\rightarrow} \mathrm{B} \qquad (3.12.1)$$

We arrive at the sub-goal of the protocol

$$\mathrm{A}\ |\equiv \mathrm{B}|\ \equiv \xrightarrow{K_A} A \qquad (2.6.1)$$

$$B|\equiv \mathrm{A}|\ \equiv \xrightarrow{K_A} \mathrm{A} \qquad (2.5.1)$$

$$\mathrm{B} \mid \equiv \mathrm{C}| \equiv \xrightarrow{K_B} B \qquad (2.12.1)$$

$$C|\equiv \mathrm{B}|\ \equiv \xrightarrow{K_B} \mathrm{B} \qquad (2.11.1)$$

Also, we arrive at the goal of the protocol

$$\mathrm{A}| \equiv \xrightarrow{K_A} \mathrm{A} \qquad (3.6.1)$$

$$\mathrm{B}| \equiv \overset{A}{\rightarrow} \mathrm{A} \qquad (3.5.1)$$

$$\mathrm{B}| \equiv \xrightarrow{K_B} \mathrm{B} \qquad (3.12.1)$$

$$\mathrm{C}| \equiv \xrightarrow{K_B} \mathrm{B} \qquad (3.11.1)$$

Hence, the protocol is secure because we arrive at the goal and sub-goal, and each principle knows the other.

4.2. Performance analysis, Attack resistance and functionality:

The attack resistance of the proposed scheme is compared with that of four other schemes as in table (1). The comparison in terms of mutual trust, Session key agree-ment, Replay attack resistance, Man-in-the-middle attack resistance, off-line diction-ary attack resistance. The comparison with Secure delegation based authentication protocol for wireless rooming service in Tsai, Lo & Wu, (2012), Trust-Based Authentication for Secure Communication in Cognitive Radio Networks in Parvin, Han, Tian & Hussain, (2010, December), A new authen-tication scheme for wireless ad hoc network in Xingliang & Shilian (2012, October), and A Dynamic

Table 1. Performance comparison

Functionally	Tsai, Lo & Wu. (2012)	Parvin, Han, Tian & Hussain. (2010, December)	Xingliang, & Shilian. (2012, October)	Wong, Zheng, Cao & Wang. (2006, June)	Proposed scheme
mutual trust	No	No	Yes	No	Yes
Session key agreement	Yes	No	Yes	No	Yes
Replay attack resistance	Yes	Yes	No	yes	Yes
Man-in-the middle attack resistance	No	No	Yes	No	Yes
off-line dictionary attack	yes	Yes	No	yes	Yes

User Authentication Scheme for Wireless Sensor Network in Wong, Zheng, Cao & Wang. (2006, June).

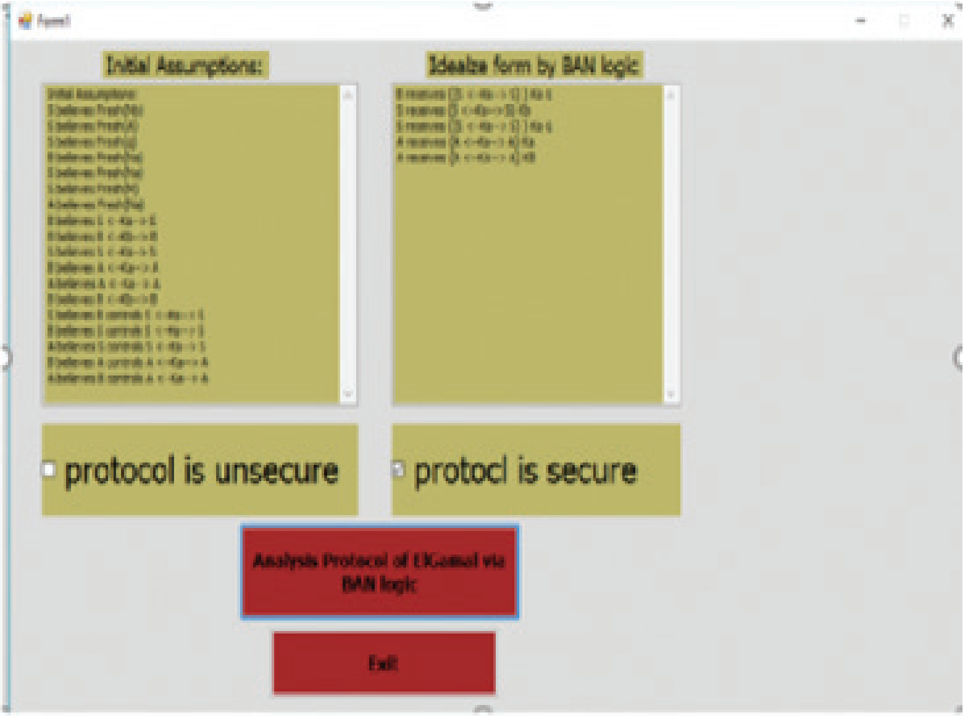
- Replay attack prevention: In a replay attack, An attacker can capture the package and resend these packets after another period (Butt, M. A., 2013). The nonce makes the message of the current communication different from the messages of past communi-cations. Therefore, the protocol is secure against replay attacks and offline dictionary attacks.

- Man-in-the-middle attack prevention: In this type of attack, the attacker tries to spy on the communication between two users communicating with each other via a net-work. A man-in-the-middle attack is not possible in the proposed method because our proposal is based on mutual authentication, in which random numbers, refreshed with each iteration of the protocol, are used.

The performance analysis shows that our proposed scheme performs better than other existing user authentication schemes.

Practical aspect:

- We are programming BAN logic depending on the environment of C# language. Moreover, apply the ElGamal protocol to the rule of BAN logic. The input is the protocol of ElGamal, rules of BAN logic, and assumptions while Output will consist of idealize form and message which proving that protocol is secure. The executing


Form1
Initial Assumptions:
Idealize form by BAN logic
Analysis Protocol of ElGamal via BAN logic
Exit

```
Initial Assumptions:
[illegible] believes Fresh([illegible])
[illegible] believes Fresh([illegible])
[illegible] believes Fresh([illegible])
[illegible] believes Fresh([illegible])
[illegible] believes Fresh([illegible])
[illegible] believes Fresh([illegible])
[illegible] believes Fresh([illegible])
[illegible] believes [illegible] <-K[illegible]-> [illegible]
[illegible] believes [illegible] <-K[illegible]-> [illegible]
[illegible] believes [illegible] <-K[illegible]-> [illegible]
[illegible] believes [illegible] <-K[illegible]-> [illegible]
[illegible] believes [illegible] <-K[illegible]-> [illegible]
[illegible] believes [illegible] <-K[illegible]-> [illegible]
[illegible] believes [illegible] controls [illegible] <-K[illegible]-> [illegible]
[illegible] believes [illegible] controls [illegible] <-K[illegible]-> [illegible]
[illegible] believes [illegible] controls [illegible] <-K[illegible]-> [illegible]
[illegible] believes [illegible] controls [illegible] <-K[illegible]-> [illegible]
[illegible] believes [illegible] controls [illegible] <-K[illegible]-> [illegible]
```

```
[illegible] receives {[illegible] <-K[illegible]-> [illegible]} [illegible]
[illegible] receives {[illegible] <-K[illegible]-> [illegible]} [illegible]
[illegible] receives {[illegible] <-K[illegible]-> [illegible]} [illegible]
[illegible] receives {[illegible] <-K[illegible]-> [illegible]} [illegible]
[illegible] receives {[illegible] <-K[illegible]-> [illegible]} [illegible]
```

☐ protocol is unsecure

☐ protocl is secure

Fig. 3: The result of executing the proposed scheme in C# programming

of the program show that this protocol is secure as in figure (2):

5. Conclusionsn

This paper proposes a security protocol for mutual authentication in cognitive radio networks, which are performing exchanged authentication between the sender and recipient. Then the data is encrypted and sent securely decrypted by the recipient and to ensure the authenticity of the work of the Protocol and the integrity of the data from the various attacks on the network. We analyzed the protocol using BAN logic which has proved that he did not prevent the attacks only, but achieved the best per-formance of the system.

References

Abadi, M., & Tuttle, M. R. (1991, August). A semantics for a logic of authentication. In *PODC* (Vol. 91, pp. 201-216).

Alhakami, W., Mansour, A., Safdar, G. A., & Albermany, S. (2013, October). A secure MAC protocol for cognitive radio networks (SMCRN). In *2013 Science and Information Conference* (pp. 796-803). IEEE.

Bhandari, S., & Moh, S. (2015). A survey of MAC protocols for cognitive radio body area networks. *Sensors, 15*(4), 9189-9209.

Burrows, M., Abadi, M., & Needham, R. M. (1989). A logic of authentication. *Proceedings of the Royal Society of London. A. Mathematical and Physical Sciences, 426*(1871), 233-271.

Butt, M. A. (2013). Cognitive radio network: Security enhancements. ***Journal of Global Research in Computer Science*, *4***(2), 36-41.

Clancy, T. C., & Goergen, N. (2008, May). Security in cognitive radio networks: Threats and mitigation. In *2008 3rd International Conference on Cognitive Radio Oriented Wireless Networks and Communications (CrownCom 2008)* (pp. 1-8). IEEE.

Elkashlan, M., Wang, L., Duong, T. Q., Karagiannidis, G. K., & Nallanathan, A. (2014). On the security of cognitive radio networks. *IEEE Transactions on Vehicular Technology, 64*(8), 3790-3795.

Idoudi, H., Daimi, K., & Saed, M. (2014, July). Security challenges in cognitive radio networks. In *Proceedings of the World Congress on Engineering* (Vol. 1, pp. 2-4).

Mishra, V., Mathew, J., & Lau, C. T. (2016). *QoS and Energy Management in Cognitive Radio Network: Case Study Approach.* Springer.

Mitola, J. I. (2002). Cognitive radio. An integrated agent architecture for software defined radio.

Mitola, J., & Maguire, G. Q. (1999). Cognitive radio: making software radios more personal. *IEEE personal communications, 6*(4), 13-18.

Parvin, S., Han, S., Tian, B., & Hussain, F. K. (2010, December). Trust-based authentication for secure communication in cognitive radio networks. In *2010 IEEE/IFIP International Conference on Embedded and Ubiquitous Computing* (pp. 589-596). IEEE.

Parvin, S., Hussain, F. K., Hussain, O. K., Han, S., Tian, B., & Chang, E. (2012). Cognitive radio network security: A survey. *Journal of Network and Computer Applications, 35*(6), 1691-1708.

Reddy, Y. B. (2013, June). Security issues and threats in cognitive radio networks. In *The ninth advanced international conference on telecommunications (AICT 2013)* (pp. 84-89).

Stallings, W. (2017). *Cryptography and network security: principles and practice* (pp. 92-95). Upper Saddle River: Pearson

Syverson, P., & Cervesato, I. (2000, September). The logic of authentication protocols. In *International School on Foundations of Security Analysis and Design* (pp. 63-137). Springer, Berlin, Heidelberg.

Tang, L., & Wu, J. (2012). Research and analysis on cognitive radio network security. *Wireless Sensor Network, 4*(04), 120.

Thakre, S., & Dixit, S. (2014). Security Threats and Detection Technique in Cognitive radio Network. *International Journal of Emerging Technology and Advanced Engineering, 4*(2).

Tsai, J. L., Lo, N. W., & Wu, T. C. (2012). Secure delegation-based authentication protocol for wireless roaming service. *IEEE Communications Letters, 16*(7), 1100-1102.

Wessels, J., & BV, C. F. (2001). Application of BAN-logic. CMG FINANCE BV, 19, 1-23.

Wong, K. H., Zheng, Y., Cao, J., & Wang, S. (2006, June). A dynamic user authentication scheme for wireless sensor networks. In *IEEE International Conference on Sensor Networks, Ubiquitous, and Trustworthy Computing (SUTC'06)* (Vol. 1, pp. 8-pp). IEEE.

Xingliang, Z., & Shilian, X. (2012, October). A new authentication scheme for Wireless Ad Hoc Network. In *2012 International Conference on Information Management, Innovation Management and Industrial Engineering* (Vol. 2, pp. 312-315). IEEE.

Zhang, N., Lu, N., Cheng, N., Mark, J. W., & Shen, X. S. (2013). Cooperative spectrum access towards secure information transfer for CRNs. *IEEE Journal on Selected Areas in Communications, 31*(11), 2453-2464.

Submitted 12.09.2019
Accepted 15.11.2019