Authentication of RSA via BAN logic

Israa N.A. Alsalhi
University of Kufa
Najaf, Iraq
israan.alsalhi@student.uokufa.edu.iq

Salah A. K. Albermany
University of Kufa
Najaf, Iraq
Salah.albermany@uokufa.edu.iq

Received Oct. 1, 2018. Accepted for publication Jan. 17, 2019

DOI : *http://dx.doi.org/10.31642/JoKMC/2018/060101*

Abstract*-Web exchanges are conducted through an open network that lacks central management; it is, therefore, impossible to identify a communication partner, especially in a distributed system. Authentication is the basis of security in such systems. Providing secure communication becomes problematic in CRN because cognitive node can join and leave network dynamically that leading to be many threats targeting this kind of network. In this paper, we are using analysis authentication protocol of RSA algorithm by BAN logic also It using C# programing . By analyzing via BAN logic, we will see if this protocol is confidential, and can it be used in cognitive radio networks.*

Keywords: Cognitive radio network; BAN logic; security; RSA

I. INTRODUCTION

The concept of CR was first presented by J. Mitola and G. Q. Maguire [1]. It is a new approach in wireless communications that Mitola later described in his doctoral dissertation [2].CR, which is built on a software-defined radio, is defined as an intelligent wireless communication system that is aware of its environment and uses the methodology of understanding by building to learn from the environment and adapt to statistical variations in the input stimuli [3] [4].The two main aims of cognitive radio are: highly reliable communication whenever and wherever needed, and efficient utilization of the radio spectrum [5]**.** CR is a novel concept because there were several problems in the wireless communication system. One of the main problems of broadband wireless communications is the limited availability of the spectrum [6] needed to provide high-speed telecommunications services at any time and anywhere [7]. The use of the licensed spectrum for most systems was found to be limited. A survey by the Federal Communications Commission (FCC) in New York for the band from 30 MHz to 3 GHz found only 13.1% spectrum utilization rate [8].

Accordingly, cognitive radio (CR) proposal was introduced to enhance the overall spectrum utilization [9] and provide adequate spectrum for broadband wireless communications

A logic for analyzing authentication protocols (BAN logic) which is a logic of belief with special features for determining some of the central authentication concepts has been proposed by Burrows, Abadi, and Needham[10]. With this logic, several errors in the published protocols have been revealed[11] . Authentication in a network system involves the determination of the identity of a character such as a computer, server or a person. It plays a vital role in system security. The principals requesting for network accessibility must be identified in one way or the other.

Authentication is mainly a secret process which relies on the use of passwords and encryption keys must be presented by an intending principal to gain access to the network facility[12]. In various branches of modern theoretical computing, the graphs and other objects derived from authentication processes are basic essential tools actively deployed in network security [13].

II. RELATED WORK

- Authentication protocols have been regarded as the foundation for security in the distributed systems which must function properly to avoid security breaches. Most of the available protocols in the literature are prone to error as they are laden with redundancies and other security flaws. With a simple logic, the belief (a consequence of communication) of trustworthy parties that take part in authentication protocols was able to be described[10].

-A dynamic strong password-based solution to access control problems is adapted to a wireless sensor network environment. The proposed strong password-based authentication approach requires simple operations, such as one-way hash function and exclusive-OR operations. This approach allows Legitimate Users (LUs) to request sensor data from any of the sensor nodes. The scheme was claimed to be secure against replay and forgery attacks [14].

- The scheme is not only retains all the advantages of the previous scheme [14], but is also modified and enhances its security. This approach also resists replay and forgery attacks, reduces a user's password leakage risk, and allows the use of changeable passwords [15].

III. BAN lOGIC

BAN logic is a highly sorted modal logic which can establish the distinction among several objects, encryption keys, principals, and formulas [16]. Being that the Needham-Schroeder and Kerberos protocols achieved their goal, their description is basically informal. A closer observation reveals that first, there are certain assumptions in the protocols such as "servers that have my password can be trusted"; and secondly, each participant in the network can make certain deductions based on the received assumptions and information [17].

In a normal situation, all the assumptions involved in a protocol can be explicitly made, and also, each protocol step can be transformed into the application of one or more general deduction rules to allow the drawing of further conclusions. The formalization of an argument involves a rigorous account of all the assumptions and steps made and expressing same symbolically so that checking becomes a mere mechanical process. The logic of authentication refers to the logical calculus which is based on an accepted set of deduction rules for formal reasoning on authentication protocols. Such logic has the following advantages[18] :

- Correctness: There should be a possibility of proving that a protocol met or did not meet its security goals. If the stated goals were not met, the logic of authentication ought to show what to be done to meet the goal
- Efficiency: If the efficiency of the protocol in the absence of some messages which are parts of a protocol, then, the efficiency of the protocol can be enhanced by eliminating such redundant messages. .
- Applicability: To decide if a protocol can be deployed in a practical situation, it helps in the clarification of the assumptions of the protocol by formally stating them. It can also be determined if any of the stated assumptions is needed to meet the authentication goals.

- Alhakami et al. (2013) proposed Secure MAC Cognitive Radio Network (SMCRN), the presented protocol is analysed for these security measures using formal logic methods such as Burrows Abadi Needham (BAN) logic. It is shown that the proposed protocol functions effectively to provide strong authentication and detection against malicious users leading to subsequent secure communication. In this way, replay attack, DoS attack, and forgery attack are reduced [19].
- Chehelcheshmeh and Hosseinzadeh (2016) presented a method for mutual authentication in centralized CRNs. The proposed scheme does not use digital certificates and thus does not have the disadvantages of public key infrastructure schemes; such as low efficiency and high costs. This method enjoys high speed, quantum security, and low costs. In this way, reflection attack, replay attack, and man in the middle attack are reduced [20].

The method and formalism of BAN logic

The analysis of any protocol using BAN logic involves three main stages; the first stage involves the expression of the goals and assumptions as formulas or statements in a symbolic notation. This is to ensure the progression of the logic from a known state and to be able to determine if the protocol reached the set goals [21]. In the second stage, there is a transformation of the protocol steps into formulas calling idealize protocol. The last stage involves the application of a set of deduction rules known as postulates. The postulates should lead from the assumptions through intermediate formulas to the authentication goals.

The analysis of a protocol is based on the perspective of each principal participant P. Each participant receives messages in relation to the previous messages he received or sent. A basic issue is a determination of which a participant should be trusted the based on the messages he sent or received [22].

The BAN logic and authentication protocol assumptions are similar as they are based on the target of analysis. Authentication is performed between trustworthy participants although this trust may be foiled by attackers via eavesdropping, message replays, or via sending of malicious messages [23].

To apply the BAN logic, the actions and messages of the participants are first transformed into formulas. The following are some basic rules for BAN logic:

Message-meaning: this rule allows the identity of the sender of an encrypted message to be deduced from the encryption key being used.

$$R1 = \frac{p \mid \equiv \; Q \overset{k}{\leftrightarrow} p, p \;\; \rhd \{x\}_k}{p \mid \equiv Q| \sim x} \qquad (1)$$

Where K is a shared key between Q and P; so, if P receives any message encrypted with K, it must have originated from Q, and P must ignore its own messages.

Nonce-verification: this rule allows the derivation of beliefs from freshly uttered messages.

$$R2 = \frac{p \mid \equiv \#(x), p \mid \equiv Q| \sim x}{p \mid \equiv Q| \equiv x} \qquad (2)$$

If P believes that Q once said X, then, P believes that Q once believed X. If X is fresh, then, Q should still hold this belief.

Jurisdiction rule: this rule allows belief based on jurisdiction to be derived. If P trusts Q as an authority on X, then, P should believe X if Q does so.

$$R3 = \frac{p \mid \equiv \; Q \overset{k}{\Rightarrow} x, p \mid \equiv Q| \equiv x}{p \mid \equiv x} \qquad (3)$$

IV. THE PROPOSED METHOD

In RSA , the sever generate two prime number p, q and send to node B. node B will be taken the following step to generate his key pair:

1. Private Key computing:

After server select two number, node B multiply the two prime number to become the first private key and the second compute it that represent as d.

2. Public key assembling n

node B selects an integer (e), 1<e< ϕ (n). We will deal with him here as public key this is the first part, while the second part yield from multiply the two number that generate by server.

4. Public key publishing

The public key now needs to be published by node B, for this reason server is able to get hold of it. As in algorithm (1)

```
Algorithm (1): Authentication using (RSA algorithm)
Input: Request from Node A and Node B.
Output: Authenticate or not.
  1-  Node A sends a request to server S to
      communicate with node B.
  2-  Server S selects two prime numbers {p, q},
      where p ≠q.
      Then, server S sends {p, q} to node B.
  3-  B=
      $\begin{cases} n = p * q \\ \text{computes } \phi(n) = (p - 1) * (q - 1) \\ \text{Select e, } \gcd(\phi(n), e) = 1{,}1 < e < \phi(n) \\ \text{compute } d = e^{-1}(\text{mod}(\phi(n)) \;\; : \text{ sends publ} \end{cases}$
  4-  Server=
      $\begin{cases} \text{public key}\{e, n\} \quad \text{and} \quad \text{sends it to node A} \\ \quad \text{sends a plain text as an integer M, } M < n \end{cases}$
  5-  A={$C = M^e \text{ mod } n \quad : \text{ sends to node B}$
  6-  B=
      $\begin{cases} M1 = C^d \text{ mod } n \\ C' = M1^e \text{ mod } n \\ \text{A is authenticate and sends } \{C'\} \text{ to node A} \quad \text{i} \\ \text{A is not authenticated} \end{cases}$
  7-  Node B sends a request to server S to
      communicate with node C.
  8-  Server S selects two prime numbers {p, q},
      where p ≠q.
      Then, server S sends {p, q} to node C.
  9-
      $\text{Node C} =$
      $\begin{cases} n = p * q \\ \text{computes } \phi(n) = (p - 1) * (q - 1) \\ \text{Select e, } \gcd(\phi(n), e) = 1{,}1 < e < \phi(n) \\ \text{compute } d = e^{-1}\text{mod}(\phi(n)) \;\; : \text{ sends publi} \end{cases}$
  10- Server=
      $\begin{cases} \text{public key}\{e, n\} \quad \text{and} \quad \text{sends it to node B} \\ \quad \text{sends a plain text as an integer M, } M < n \end{cases}$
  11- B={$C = M^e \text{ mod } n \quad : \text{ sends to node C}$
  12- $\text{Node C} =$
      $\begin{cases} M1 = C^d \text{ mod } n \\ C' = M1^e \text{ mod } n \\ \text{B is authenticate and sends } \{C'\} \text{ to node B} \quad \text{i} \\ \text{B is not authenticated} \end{cases}$
```

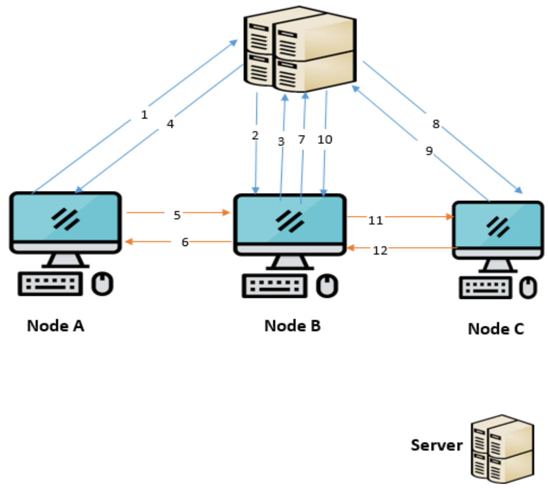


Figure 1: Authentication using (RSA algorithm)

The original message of authentication phase are representing as follow:

MSG 1: A → S: A, B from CHs

MSG 2: S → B: $\{N_B$, # (p, q), $K_S\}_{KS}{}^{-1}$ from S

MSG 3: B → S: $\{N_A$, N, auler, #e, d, K_S, $A\}_{KB}$ from B

MSG 4: S → A: $\{N_A$,# (M) , K_S ,B } $_{KS}{}^{-1}$ from S

MSG 5: A → B: $\{N_A$, C, $K_{A,}$,$A\}_{KA}$ from A

MSG 6: B → A: {M1, $K_A\}_{KB}$ from B

MSG 7: B → S: B, C from CHs

MSG 8: S → C: $\{N_c$, # (p, q), $K_S\}_{KS}{}^{-1}$ from S

MSG 9: C → S: $\{N_B$, N, auler, #e, d, K_S, $B\}_{KC}$ from B

M'SG 10 : S → B: { N_B ,# (M) , K_S ,C } $_{KS}{}^{-1}$ from S

MSG 11: B → C: $\{N_B$, C, $K_{B,}$ $B\}_{KB}$ from A

MSG 12: C → B: {M1, $K_B\}_{KC}$ from B

V. PROTOCOL ANALYSIS BY BAN LOGIC

We are analyzing authentication phase of RSA algorithm. The idealized protocol is 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 ⊳ { N_B ,# (p , q), $\overset{KS}{\rightarrow}S\}_{KS}{}^{-1}$ from S

MSG 3 : S ⊳{ N_A , N, auler, #e ,d , $\overset{KS}{\rightarrow}$S} $_{KB}$ from B

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

MSG 5 : B ⊳{ N_A , C, $\overset{KA}{\rightarrow}$A} $_{KA}$ from A

MSG 6 : A ⊳ { M1 , $\overset{KA}{\rightarrow}$A } $_{KB}$ from B

MSG 8 : C ⊳ { N_c , # (p, q) , K_S $\}_{KS}{}^{-1}$ from S

MSG 9 : S ⊳ { N_B, N, auler, #e ,d , K_S, $B\}_{KC}$ from B

MSG 10 : B ⊳ { N_B ,# (M) , K_S ,C } $_{KS}{}^{-1}$ from S

MSG 11 :C ⊳{ N_B, C, $K_{B,}$,$B\}_{KB}$ from A

MSG 12 : B ⊳ { M1, $K_B\}_{KC}$ from B

State assumption about original message

$S| \# N_B$ (4.1)

$S| \equiv \# M$ (4.2)

$S| \equiv \# p$ (4.3)

$A| \equiv \# q$ (4.4)

$A| \equiv \# N_A$ (4.5)

$B| \equiv \# NA$ (4.6)

$B| \equiv \# e$ (4.7)

$S| \equiv \# Na$ (4.8)

$B| \equiv \overset{KA}{\rightarrow} A$ (4.9)

$S| \equiv \overset{K_S}{\rightarrow} S$ (4.10)

$B| \equiv \overset{KS}{\rightarrow} S$ (4.11)

$S| \equiv \overset{KB}{\rightarrow} B$ (4.12)

$B| \equiv \# Na$ (4.13)

$A| \equiv \overset{KA}{\rightarrow} A$ (4.14)

$A| \equiv \overset{KB}{\rightarrow} B$ (4.15)

$B| \equiv \overset{K_B}{\rightarrow} B$ (4.16)

$C| \# NB$ (4.17)

$B \mid \equiv S \Longrightarrow \overset{KS}{\rightarrow} S$ (4.18)

$S \mid \equiv B \Longrightarrow \overset{KS}{\rightarrow} S$ (4.19)

$A \mid \equiv S \Longrightarrow \overset{KS}{\rightarrow} S$ (4.20)

$B \mid \equiv A \Longrightarrow \overset{KA}{\rightarrow} A$ (4.21)

$A \mid \equiv B \Longrightarrow \overset{K_B}{\rightarrow} B$ (4.22)

$C \mid \equiv S \Longrightarrow \overset{KS}{\rightarrow} S$ (4.23)

$C| \equiv \overset{K_S}{\rightarrow} S$ (4.24)

$S| \equiv \overset{KC}{\rightarrow} C$ (4.25)

$S| \equiv \# Nc$ (4.26)

$S \mid \equiv C \Longrightarrow \overset{KS}{\rightarrow} S$ (4.27)

$B| \equiv \overset{K_C}{\rightarrow} C$ (4.28)

$C| \equiv \overset{kB}{\rightarrow} B$ (4.29)

$C \mid \equiv \ B \Rightarrow \overset{KB}{\rightarrow} B$ (4.30)

$B| \equiv \# \, Nc$ (4.31)

$B \mid \equiv \ C \Rightarrow \overset{K_C}{\rightarrow} C$ (4.32)

Apply rules:

MSG 2 B ⊳ {N_B ,# (p , q), $\overset{KS}{\rightarrow}$S}$_{KS}^{-1}$from S

$R1$

$$= \frac{B| \equiv \overset{K_S}{\rightarrow} S \, , B \ \rhd \{ \, NB \, , \# \, (\, p \, , q \,), \overset{KS}{\rightarrow} B\} KS^{-1}}{B \mid \equiv S| \sim \overset{K_S}{\rightarrow} S} \quad (1.1)$$

$$R2 = \frac{B \mid \equiv \#(NA), B \mid \equiv S| \sim \overset{K_S}{\rightarrow} S}{B \mid \equiv S| \equiv \overset{K_S}{\rightarrow} S} \qquad (2.1)$$

$$R3 = \frac{B \mid \equiv \ S \Rightarrow \overset{KS}{\rightarrow} S \ \ B \mid \equiv S| \equiv \overset{K_S}{\rightarrow} S}{B| \equiv \overset{KS}{\rightarrow} S} \qquad (3.1)$$

The result are:

$B \mid \equiv S| \equiv \overset{K_S}{\rightarrow} S$ (2.1.1)

$B| \equiv \overset{KS}{\rightarrow} S$ (3.1.1)

MSG 3 : S ⊳ { N_A , N, auler,,#e ,d , $\overset{KS}{\rightarrow}$S} $_{KB}$ from B

$R1$

$$= \frac{S| \equiv \overset{KB}{\rightarrow} B \ \ , \left\{ NA \, , , N, auler, \#e \, , d \ \ , \overset{KS}{\rightarrow} S \right\} KB}{S \mid \equiv B| \sim \overset{KS}{\rightarrow} S} \quad (1.1)$$

$$R2 = \frac{S \mid \equiv \#(NB), S \mid \equiv B| \sim \overset{KS}{\rightarrow} S}{S \mid \equiv B| \equiv \overset{KS}{\rightarrow} S} \qquad (2.1)$$

$$R3 = \frac{S \mid \equiv \ B \Rightarrow \overset{KS}{\rightarrow} S \, , S \mid \equiv B| \sim \overset{KS}{\rightarrow} S}{S| \equiv \overset{KS}{\rightarrow} S} \qquad (3.1)$$

The result are:

$S \mid \equiv B| \equiv \overset{KS}{\rightarrow} S$ (2.1.1)

$S| \equiv \overset{KS}{\rightarrow} S$ (3.1.1)

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

$R1$

$$= \frac{A| \equiv \overset{kS}{\rightarrow} S, \ \ A \ \rhd \ \{ \, NA, \#(\, M \,) \, , \overset{KS}{\rightarrow} S \, \} \, KS^{-1}}{A \mid \equiv S| \sim \overset{KS}{\rightarrow} S} \quad (1..1)$$

$$R2 = \frac{A \mid \equiv \#(NA), A \mid \equiv S| \ \sim \overset{KS}{\rightarrow} S}{A \mid \equiv S| \equiv \overset{KS}{\rightarrow} S} \qquad (2.1)$$

$$R3 = \frac{A \mid \equiv \ S \Rightarrow \overset{KS}{\rightarrow} S \, , A \mid \equiv S| \equiv \overset{KS}{\rightarrow} S}{A \equiv \overset{KS}{\rightarrow} S} \qquad (3.1)$$

The result are:

$A \mid \equiv S| \equiv \overset{KS}{\rightarrow} S$ (2.1.1)

$A \equiv \overset{KS}{\rightarrow} S$ (3.1.1)

MSG 5 : B ⊳ { N_A , C $\overset{KA}{\rightarrow}$A} $_{KA}$ from A

$$R1 = \frac{B| \equiv \overset{kA}{\rightarrow} A \, , \ B \ \rhd \ \{ \, NA \, , C \ \overset{KA}{\rightarrow} A\} \, KA}{B \mid \equiv A| \sim \overset{K_A}{\rightarrow} A} \qquad (1.1)$$

$$R2 = \frac{B \mid \equiv \#(NA), B \mid \equiv A| \sim \overset{K_A}{\rightarrow} A}{B \mid \equiv A| \equiv \overset{K_A}{\rightarrow} A} \qquad (2.1)$$

$$R3 = \frac{B \mid \equiv \ A \Rightarrow \overset{KA}{\rightarrow} A \, , B \mid \equiv A| \equiv \overset{K_A}{\rightarrow} A}{B| \equiv \overset{K_A}{\rightarrow} A} \qquad (3.1)$$

The result are:

$B \mid \equiv A| \equiv \overset{K_A}{\rightarrow} A$ (2.1.1)

$B| \equiv \overset{K_A}{\rightarrow} A$ (3.1.1)

MSG 6 : A ⊳ {M1 ,$\overset{K_A}{\rightarrow} A$ } $_{KB}$ from B

$$R1 = \frac{A| \equiv \overset{K_B}{\rightarrow} B \, , A \ \rhd \ \left\{ M1, \overset{K_A}{\rightarrow} A \right\} KB}{A \mid \equiv B| \sim \overset{K_A}{\rightarrow} A} \qquad (1.1)$$

$$R2 = \frac{A \mid \equiv \#(NA), A \mid \equiv B| \sim \overset{K_A}{\rightarrow} A}{A \mid \equiv B| \equiv \overset{K_A}{\rightarrow} A} \qquad (2.1)$$

$$R3 = \frac{A \mid \equiv \ B \Rightarrow \overset{K_B}{\rightarrow} B \, , A \mid \equiv B| \equiv \overset{K_A}{\rightarrow} A}{A| \equiv \overset{kA}{\rightarrow} A} \qquad (3.1)$$

The result are:

$A \mid \equiv B| \equiv \overset{K_A}{\rightarrow} A$ (2.1.1)

$A| \equiv \overset{K_A}{\rightarrow} A$ (3.1.1)

MSG 8 : C ⊳ { N_c , # (p, q) , K_S }$_{KS}^{-1}$ from S

$R1$

$$= \frac{C| \equiv \overset{K_S}{\rightarrow} S \, , C \ \rhd \ \{ \, Nc \, , \ \# \, (\, p, q \,) \, , KS \, \} KS^{-1}}{C| \equiv S| \sim \overset{K_S}{\rightarrow} S} \quad (1.1)$$

$$R2 = \frac{C \mid \equiv \#(NB), C| \equiv S| \sim \overset{K_S}{\rightarrow} S}{C| \equiv S| \equiv \overset{K_S}{\rightarrow} S} \qquad (2.1)$$

$$R3 = \frac{C \mid \equiv \ S \Rightarrow \overset{KS}{\rightarrow} S, C| \equiv S| \equiv \overset{K_S}{\rightarrow} S}{C| \equiv \overset{KS}{\rightarrow} S} \qquad (3.1)$$

The result are:

$C \mid \equiv S| \equiv \overset{K_S}{\rightarrow} S$ (2.1.1)

$C| \equiv \overset{KS}{\rightarrow} S$ (3.1.1)

MSG 9 : S ⊳ { N_B, N, auler, #e ,d , K_S, B}$_{KC}$ from C

$R1$

$$= \frac{S| \equiv \overset{KC}{\rightarrow} C \ \ , S \ \rhd \ \{ \, NB, N, auler, \#e \, , d \ \ , KS, B\} KC}{S \mid \equiv C| \sim \overset{KS}{\rightarrow} S} \, (1.1)$$

$$R2 = \frac{S \mid \equiv \#(NC), S \mid \equiv C| \sim \overset{KS}{\rightarrow} S}{S \mid \equiv C| \equiv \overset{KS}{\rightarrow} S} \qquad (2.1)$$

$$R3 = \frac{S \mid \equiv \ C \Rightarrow \overset{KS}{\rightarrow} S \, , S \mid \equiv C| \equiv \overset{KS}{\rightarrow} S}{S| \equiv \overset{KS}{\rightarrow} S} \qquad (3.1)$$

The result are:

$S \mid \equiv C| \equiv \overset{KS}{\rightarrow} S$ (2.1.1)

$$S| \equiv \overset{KS}{\rightarrow} S \qquad (3.1.1)$$

MSG 10 : $B \rhd \{ N_B ,\#(M), K_S ,C \}_{KS^{-1}}$ from S

$$R1 = \frac{B| \equiv \overset{kS}{\rightarrow} S, \quad B \rhd \{ NB ,\#(M), KS ,C \} KS^{-1}}{B |\equiv S| \sim \overset{KS}{\rightarrow} S} \quad (1.1)$$

$$R2 = \frac{B | \equiv \#(NB), B | \equiv S| \sim \overset{KS}{\rightarrow} S}{B | \equiv S| \equiv \overset{KS}{\rightarrow} S} \qquad (2.1)$$

$$R3 = \frac{B | \equiv S \Rightarrow \overset{KS}{\rightarrow} S , B | \equiv S| \equiv \overset{KS}{\rightarrow} S}{B \equiv \overset{KS}{\rightarrow} S} \qquad (3.1)$$

The result are:

$$B |\equiv S| \equiv \overset{KS}{\rightarrow} S \qquad (2.1.1)$$

$$B \equiv \overset{KS}{\rightarrow} S \qquad (3.1.1)$$

MSG 11: $C \rhd \{ N_B, C, K_{B,},B\}_{KB}$ from B

$$R1 = \frac{C| \equiv \overset{kB}{\rightarrow} B , C \rhd \{ NB, C, KB,, B\}KB}{C | \equiv B| \sim \overset{K_B}{\rightarrow} B} \qquad (1.1)$$

$$R2 = \frac{C | \equiv \#(NB), C | \equiv B| \sim \overset{K_B}{\rightarrow} B}{C | \equiv B| \equiv \overset{K_B}{\rightarrow} B} \qquad (2.1)$$

$$R3 = \frac{C | \equiv B \Rightarrow \overset{KB}{\rightarrow} B , C | \equiv B| \equiv \overset{K_B}{\rightarrow} B}{C| \equiv \overset{K_B}{\rightarrow} B} \qquad (3.1)$$

The result are:

$$C | \equiv B| \equiv \overset{K_B}{\rightarrow} B \qquad (2.1.1)$$

$$C| \equiv \overset{K_B}{\rightarrow} B \qquad (3.1.1)$$

MSG 12 : $B \rhd \{ M1, K_B\}_{KC}$ from B

$$R1 = \frac{B| \equiv \overset{K_C}{\rightarrow} C , B \rhd \{ M1, KB\}KC}{B | \equiv C| \sim \overset{K_B}{\rightarrow} B} \qquad (1.1)$$

$$R2 = \frac{B | \equiv \#(NB), B | \equiv C| \sim \overset{K_B}{\rightarrow} B}{B | \equiv C| \equiv \overset{K_B}{\rightarrow} B} \qquad (2.1)$$

$$R3 = \frac{B | \equiv C \Rightarrow \overset{K_C}{\rightarrow} C , B | \equiv C| \equiv \overset{K_B}{\rightarrow} B}{B| \equiv \overset{kB}{\rightarrow} B} \qquad (3.1)$$

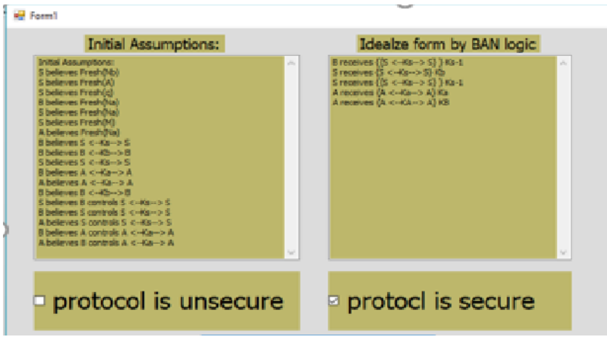
The result are:

$$B| \equiv \overset{kB}{\rightarrow} B \qquad (2.1.1)$$

$$B |\equiv C| \equiv \overset{K_B}{\rightarrow} B \qquad (3.1.1)$$

I. APPLICATION PROGRAM

C# programming is used in this section. The design has a simple and friendly user interface. The input are messages of four protocols and rules of BAN logic while output will consist of assumptions, idealize form, and secure message of each protocol after reach the goal. The result shows that RSA authentication protocol is secure as shown in Figure (2)



Initial Assumptions:

Initial Assumptions:
S believes Fresh(Nb)
S believes Fresh(A)
S believes Fresh(c)
B believes Fresh(Na)
S believes Fresh(Na)
S believes Fresh(M)
A believes Fresh(Na)
B believes S <--Ks--> S
B believes B <--Kb--> B
S believes S <--Ks--> S
B believes A <--Ka--> A
A believes A <--Ka--> A
B believes B <--Kb--> B
S believes B controls S <--Ks--> S
B believes S controls S <--Ks--> S
A believes S controls S <--Ks--> S
B believes A controls A <--Ka--> A
A believes B controls A <--Ka--> A

Idealze form by BAN logic

B receives {(S <--Ks--> S} } Ks-1
S receives {S <--Ks--> S} Kb
S receives {(S <--Ks--> S} } Ks-1
A receives {A <--Ka--> A} Ka
A receives {A <--KA--> A} KB

☐ protocol is unsecure

☑ protocl is secure

II. CONCLOSION

Authentication is an important issue in CRN and the aim is to prevent unauthorized use of spectrum bands by malicious user. For this, cryptographic authentication mechanism can be applied for verifying the user. When analyzing the authentication of RSA algorithm by BAN logic of each the message, we are proving that it is secure, So it can be used it in cognitive radio network.

REFRENAES

[1] J. Mitola and G. Q. Maguire, “Cognitive radio: making software radios more personal,” *IEEE Pers. Commun.*, vol. 6, no. 4, pp. 13–18, 1999.

[2] J. Mitola, “Cognitive radio---an integrated agent architecture for software defined radio,” 2000.

[3] S. Haykin, “Cognitive radio: brain-empowered wireless communications,” *IEEE J. Sel. areas Commun.*, vol. 23, no. 2, pp. 201–220, 2005.

[4] A. M. Wyglinski, M. Nekovee, and T. Hou, *Cognitive radio communications and networks: principles and practice*. Academic Press, 2009.

[5] E. Hossain, D. Niyato, and Z. Han, *Dynamic spectrum access and management in cognitive radio networks*. Cambridge university press, 2009.

[6] S. X. Ting, Z. Z. Hui, and L. Y. Gang, “Spectrum consideration for wireless communications in the twenty first century,” in *Environmental Electromagnetics, 2000. CEEM 2000. Proceedings. Asia-Pacific Conference on*, 2000, pp. 29–32.

[7] J. T. J. Penttinen, *The telecommunications handbook: Engineering guidelines for fixed, mobile and satellite systems*. John Wiley & Sons, 2015.

[8] H. F. Rashvand, *Using cross-layer techniques for communication systems*. IGI Global, 2012.

[9] F. Li, Z. Li, G. Li, F. Dong, and W. Zhang, “Efficient Wideband Spectrum Sensing with Maximal Spectral Efficiency for LEO Mobile Satellite Systems,” *Sensors*, vol. 17, no. 1, p. 193, 2017.

[10] M. Burrows, M. Abadi, and R. M. Needham, “A logic of authentication,” in *Proceedings of the Royal Society of London A: Mathematical, Physical and Engineering Sciences*, 1989, vol. 426, no. 1871, pp. 233–271.

[11] M. Abadi and M. R. Tuttle, “A semantics for a logic of authentication,” in *Proceedings of the tenth annual ACM symposium on Principles of distributed computing*, 1991, pp. 201–216.

[12] K. Brauer, “Authentication and security aspects in an international multi-user network,” 2011.

[13] R. Feng, L. Hu, and J. H. Kwak, “Authentication codes and bipartite graphs,” *Eur. J. Comb.*, vol. 29, no. 6, pp. 1473–1482, 2008.

[14] K. H. M. Wong, Y. Zheng, J. Cao, and S. Wang, “A dynamic user authentication scheme for wireless sensor networks,” in *Sensor Networks, Ubiquitous, and Trustworthy Computing, 2006. IEEE International Conference on*, 2006, vol. 1, p. 8–pp.

[15] H.-R. Tseng, R.-H. Jan, and W. Yang, “An improved dynamic user authentication scheme for wireless sensor networks,” in *Global Telecommunications Conference, 2007. GLOBECOM’07. IEEE*, 2007, pp. 986–990.

[16] D. Monniaux, “Analysis of cryptographic protocols using logics of belief: an overview,” *J. Telecommun. Inf. Technol.*, pp. 57–67, 2002.

[17] J. Glasgow, G. MacEwen, and P. Panangaden, “A logic for reasoning about security,” *ACM Trans. Comput. Syst.*, vol. 10, no. 3, pp. 226–264, 1992.

[18] G. Coulouris, J. Dollimore, and T. Kindberg, “Archive Material from Edition 2 of Distributed Systems: Concepts and Design,” 1994.

[19] W. Alhakami, A. Mansour, G. A. Safdar, and S. Albermany, “A secure MAC protocol for cognitive radio networks (SMCRN),” in *Science and Information Conference (SAI), 2013*, 2013, pp. 796–803.

[20] S. Bakhtiari Chehelcheshmeh and M. Hosseinzadeh, “Quantum- resistance authentication in centralized cognitive radio networks,” *Secur. Commun. Networks*, vol. 9, no. 10, pp. 1158–1172, 2016.

[21] A. D. Rubin and P. Honeyman, “Formal methods for the analysis of authentication protocols,” Center for Information Technology Integration, 1993.

[22] P. Syverson, “The use of logic in the analysis of cryptographic protocols,” in *Research in Security and Privacy, 1991. Proceedings., 1991 IEEE Computer Society Symposium on*, 1991, pp. 156–170.

[23] S. Older and S.-K. Chin, “Formal methods for assuring security of protocols,” *Comput. J.*, vol. 45, no. 1, pp. 46–54, 2002.