Proceedings of the 5th WSEAS International Conference on Telecommunications and Informatics, Istanbul, Turkey, May 27-29, 2006 (pp321-329)

WSEAS

A bidirectional Bluetooth authentication scheme based on game-theoretic framework

Nabil El Kadhi* Syrine Karoui*† Fouad Ben Abdelaziz†‡

*LERIA, Ecole Pour l'Informatique et les nouvelles TECHnologies
24, Rue Pasteur - 94270 Le Kremlin Bicêtre - Métro: Porte d'Italie - France
Tel.: +33144080128, Fax: +33144080120

† LARODEC, Institut Supérieur de Gestion de Tunis
41, Rue de la libérté - Cité de la Bouchoucha - Le Bardo 2000 - Tunisie
Tel.: +21698695233, Fax: +21671568767

‡Visiting at Olayan School of Business, American University of Beirut (AUB)
P.O. BOX 11-0236, Riad El Solh - Beirut 1107 2020 - Lebanon
Tel.: +9611374444, Fax: +9611750214

Key words: Bluetooth security, Bluetooth authentication, game theory, Nash equilibrium.

Proceedings of the 5th WSEAS International Conference on Telecommunications and Informatics, Istanbul, Turkey, May 27-29, 2006 (pp321-329)

Abstract

We present a new Bluetooth authentication model using some game theory concepts. Bluetooth is a wireless communication protocol designed for WPAN (Wireless Personal Area Nework) use. Game theory is a branch of mathematics and logic which deals with the analysis of games. An authentication between two Bluetooth devices is an unidirectional challenge-response procedure and consequently, have many vulnerabilities. We propose a bidirectional authentication scheme. We consider the authentication as a noncooperative non-zero-sum bimatrix game. We define three strategies for each player and we compute the best-response strategies (also called Nash equilibria) for our game. Using *Simplex* algorithm, we find only one Nash equilibrium corresponding to the case where both Bluetooth devices are authentic and trying to securily communicate together. In a Nash equilibrium no player has an incentive to deviate from such situation.

Introduction

The explosive growth of electronic connectivity and wireless technologies revolutionized our society. Bluetooth is one of these technologies. It is a recently proposed standard [8] that allows for local wireless communication and facilitates the physical connection of different devices [2]. Unfortunately, this wireless environment attracted many malicious individuals. Wireless networks are exposed to many risks and hackers attacks, going from data manipulation and eavesdropping to viruses. Thus, the need of security is more and more vital.

In other hands, many security problems have been addressed by game theory. In fact, game theory is the formal study of interactive decision processes [11]. It enhances the understanding of conflict and cooperation by mathematical models and abstractions.

1 Related work

Bluetooth networks are proliferating in our society. Unfortunately, the Bluetooth security has many weaknesses. Del Vecchio and El Kadhi [8] explain many attacks based on the Bluetooth protocol and on Bluetooth software implementations.

The application of game theory to networks security has been gaining increasing interest within the past few years. For example, Syverson [14] talks about "good" nodes fighting "evil" nodes in network and suggests using game theory for reasoning. In [3], Browne describes how game theory can be used to analyze attacks involving complicated and heterogeneous military networks. Buike [4] studies the use of games to model attackers and defenders in information warfare.

In this work, we focus on the vulnerability of the Bluetooth authentication. Since such process is unilateral, a malicious Verifier can considerably damage his correspondent menacing the operability of that device on the one hand and, the confidentiality and the integrity of the data exchanged on the other hand. To counter this weakness, we use a game-theoretic framework to model a bidirectional authentication between two Bluetooth devices. Using the Nash equilibrium concept, we define a secure authentication process where the authentication is successfull if and only il both devices are trusted. This paper is structured as following. First, we rewiew the Bluetooth protocol and focus on its security procedures and vulnerabilities in section 2. Then, section 3 is dedicated to a background on game theory. Next, in section 4 we move to our game-theoretic model. Our results are presented in section 5. Finally, our bidirectional Bluetooth authentication protocol is described in section 6.

2 An overview of the Bluetooth security

2.1 Bluetooth technology

Bluetooth is a short-range wireless cable replacement technology. It was researched and developed by an international group called the Bluetooth Special Interest Group (SIG). It has been chosen to serve as the baseline of the IEEE (Institute of Electronic and Electrical Engineers) 802.15.1 standard for Wireless Personal Area Networks (WPANs) [6]. Bluetooth communication adopts a master-slave architecture to form restricted types of ad-hoc networks (a collection of nodes that do not need to rely on a predifined infrastructure to keep the network connected) called piconets. A Bluetooth piconet can consist of eight devices, of which one is the master and the other are

slaves. Each device may take part in three piconets at most, but a device may be master in one piconet only. Several connected piconets form so called scatternet.

One of the main practical applications of Bluetooth technology include the ability to transfer files, audio data and other objects, such as electronic business cards, between physically disparate devices such as cell phones and PDAs (Personal Digital Assistant) or laptop. In addition, the piconets formed by Bluetooth can be useful for example in a meeting, where all participants have their own Bluetooth-compatible laptops, and want to share files with each other.

2.2 Bluetooth link-level security

The Bluetooth specification includes security features at the link level. These features are based on a secret link key that is shared by a pair of devices. Bluetooth link-level security supports key management, authentication and encryption [10].

2.2.1 Security entities

In every Bluetooth device there are four entities used for managing and maintaining security at the link level, namely [7]:

- The Bluetooth device address (BD_ADDR).
- The private link key.
- The private encryption key.
- A random number (RAND).

There is also a Bluetooth Personal Identification Number (PIN) used for authentication and to generate the initialisation key before exchanging link keys [13].

2.2.2 Key management

A key management scheme is used to generate, store, and distribute keys for the purpose of encryption, authentication and authorization [13][5]. Bluetooth specifies five different types of keys; four link keys (initialisation key, unit key, combination key and master key) [7][13] and one encryption key [5].

2.2.3 Authentication

Bluetooth authentication uses a challenge-response scheme, which checks whether the other party knows the link key [9]. Thus one device adopts the role of the Verifier and the other the role of the Claimant [7]. Authentication is unilateral, i.e. one device (the Claimant) authorises itself to another device (the Verifier). If mutual authentication is required, the authentication process is repeated with the roles exchanged [15].

The authentication process is shown in figure 1:

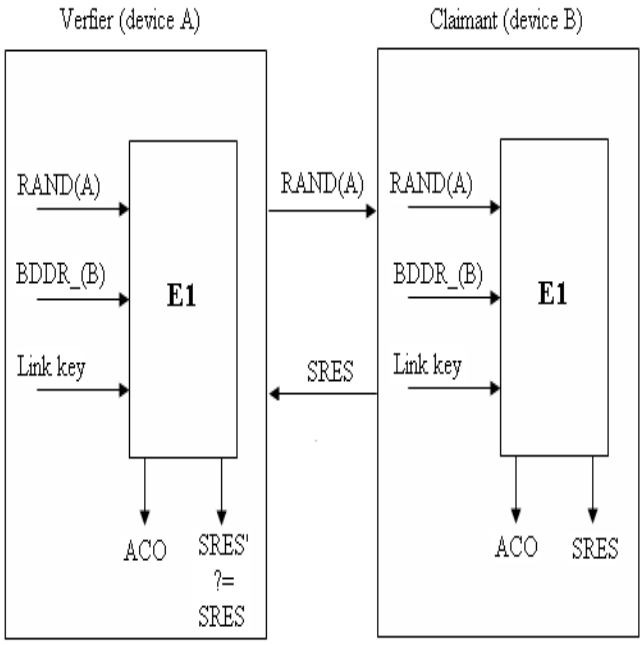

Figure 1: The authentication process [7].

2.2.4 Encryption

The encryption procedure follows on from the authentication procedure. After the link key has been determined, and authentication is successful, the encryption key is generated by the Bluetooth E3 algorithm [9][12]. The stream cipher algorithm, E0, is used for Bluetooth packet encryption and consists of three elements: the keystream generator, the payload key generator and the encryption/decryption component [7].

3 Game theory

Game theory is a systematic and formal representation of the interaction among a group of rational agents (people, corporations, animals, ...). It attempts to determine mathematically and logically the actions that players should take in order to optimize theirs outcomes.

We distinguish two main types of game-theoretic models: the strategic (or static) games and the extensive games. The strategic form (also called normal form) is a basic model studied in noncooperative game theory. A game in strategic form is given by a set of strategies for each player, and specifies the payoff for each player resulting from each strategy profile (a combination of strategies, one for each player). Each player chooses his plan of action once and for all and all players make their decisions simultaneously at the beginning of the game. When there are only two players, we can represent the strategic form game by a matrix (called bimatrix). The solution of a strategic game is a Nash equilibrium. Every strategic game with finite number of players, each with a finite set of actions has an equilibrium point. This Nash equilibrium is a point from which no single player wants to deviate unilaterally. By contrast, the model of an extensive game specifies the possible orders of the events. The players can make decisions during the game and they can react to other players' decisions. Extensive games can be finite or infinite. An extensive game is a detailed description of the sequential structure of the decision problems encountered by the players in a strategic situation.

4 Proposed model: a game-theoretic protocol

4.1 Assumptions and notations

We model the bidirectional Bluetooth authentication between two devices as a noncooperative and non-zero-sum game for two players in normal form representation (a bimatrix game). Our game is a noncooperative one because the authentication procedure is considered under the wort-case assumption. In other words, the Verifier device and the Claimant one are assumed in conflict because each of them has to consider that the other may be a malicious one. In other hands, both devices are assumed triying to reach the same optimum: communicate together without any risk. Thus, what one device gains is not necessarily what the other losts. This yields to a non-zero-sum game.

We define three strategies for each player i, $i = \{v, c\}$ (v referring to the Verifier and c referring to the Claimant):

- T_i: Say the truth and communicate with the player j.
- I_i: Say the truth and don't communicate with the player j.
- L_i: Lie and try to damage the player j.

where $j = \{v, c\}$ and $i \neq j$.
To allow only secure devices to communicate together, we affect some reward and cost values defining an utility function u_i for each player i. In practice, each strategy choice is assigned by some value of players' utility functions. The set of strategies' values is determined according to statistical computations, empirical studies, or represents values specified by the users. In our work, we choose these values according to a set of rules defining a secure bidirectionnal Bluetooth authentication. Note that we specified these rules referring to the authentication game context and logic. Thus, we have:

Rule 1 *A bidirectionnal authentication between two Bluetooth devices is secure if and only if both devices are trusted.*

Rule 2 *A Bluetooth device is winner when it is trusted and is loser otherwise.*

Rule 3 *A bidirectionnal Bluetooth authentication between two Bluetooth devices is successfull if and only if it is secure and both devices cooperate together.*

In addition, we give these assumptions to illustrate our authentication game:

Assumption 1 *Each player knows that his correspondent may be trusted device or malicious one (note that this assumption will justify the use of cryptographic parameters in our model in the sequel).*

Assumption 2 *Each player knows that if he cooperates, in others words if he says the truth and communicate with his correspondent, he will win some value ω in the best case (when his correspondent is trusted) and he will lose some value ξ on the worst-case (when his correspondent is malicious).*

Assumption 3 *Each player knows that if he tries to damage his correspondent, in others words if he lies, he will lose some value κ when his correspondent is trusted and he will win some value ι when his correspondent is malicious.*

Assumption 4 *Each player knows that he has better to be trusted in any case: $\omega > \iota$, $\xi < \kappa$ and $(\omega + \xi) > (\iota + \kappa)$.*

Assumption 5 *Each player knows that if he don't cooperate, in other words if he says the truth and don't communicate with his correspondent, he will neither win nor loose nothing.*

4.2 Costs and rewards

Next, we define the meaning of win (or reward) and loss (or cost) for the Bluetooth devices. We consider each player payoff as a function of an energy class constant G and a trust level constant Q. In fact, the Bluetooth devices need to save power to operate and the trust level of a device define the interoperability authorisation. Then, we define our utility function as following:

$$u_i = \alpha_i G - \beta_i Q$$

For each player, the term $\alpha_i G$ define the reward value whereas the term $\beta_i Q$ define the cost value. α_i value depends only on the truthworthiness of the player i. Whereas β_i depends on the truthworthiness of both players i and j. For example, if a player i is a trusted one and faces an untrusted correspondent j, i will be rewarded for his authenticity but it should pay for the non authentcity of j. Thus, we define the following values for the coefficients α_i and β_i:

$$\alpha_i = \begin{cases} 5 & \text{if } s_i = T_i \\ 5 & \text{if } s_i = L_i \\ 0 & \text{if } s_i = I_i \end{cases}$$

$$\beta_i = \begin{cases} 0 & \text{if } s_i = T_i \text{ and } s_j = T_j \\ 6 & \text{if } s_i = T_i \text{ and } s_j = L_j \\ 0 & \text{if } s_i = T_i \text{ and } s_j = I_j \\ 8 & \text{if } s_i = L_i \text{ and } s_j = T_j \\ 1 & \text{if } s_i = L_i \text{ and } s_j = L_j \\ 0 & \text{if } s_i = L_i \text{ and } s_j = I_j \\ 0 & \text{if } s_i = I_i \text{ and } s_j = I_j \end{cases}$$

where $i = \{v, c\}$, $j = \{v, c\}$, $i \neq j$, $s_i \in S_i$ (the set of player i's strategies) and u_i = the player i utility function.

4.3 The Nash equilibrium of our game

To achieve a secure bidirectional Bluetooth authentication preserving the confidentiality and the integrity of the data in transit, we use the Nash equilibrium theorem:

Theorem 1 *A Nash equilibrium of a strategic-form game is a mixed-strategy profile $\sigma^* \in \Sigma$ such that "every player is playing a best response to the strategy choices of his opponents". More formally, we say that σ^* is a Nash equilibrium if*

$$(\forall i \in P) \quad \sigma_i^* \text{ is a best response to } \sigma_{-i}^*, \qquad (1)$$

or, equivalently,

$$(\forall i \in P)(\forall s_i \in S_i) \quad u_i(\sigma_i^*, \sigma_{-i}^*) \geq u_i(s_i, \sigma_{-i}^*). \quad (2)$$

where $P = \{1, \ldots, n\}$= the player set,
S_i= Player i's pure-strategy space,
$\sum_i$= Player i's mixed-strategy space (the set of probability distributions over S_i),
$-i$= The set $P \backslash i$,
σ_i= Player i's mixed-strategy profile, and
$u_i(\sigma)$= Player i expected utility from a mixed-strategy profile σ.

To compute the Nash equilibrium of our game, we first formulate the Verifier's and the Claimant's mixed-strategy best-responses' correspondences (respectively, $MBR_V(r, s)$ and $MBR_C(p, q)$):

$$MBR_V(r,s) = \begin{cases} \{(1,0,0)\} & r > \frac{3}{8}s \text{ and } r > \frac{1}{5}s, \\ \{(0,1,0)\} & r < \frac{3}{8}s \text{ and } r < \frac{4}{3}s, \\ \{(0,0,1)\} & r < \frac{1}{5}s \text{ and } r > \frac{4}{3}s, \\ \{(p,1-p,0)\} & r = \frac{3}{8}s, \\ \{(p,0,1-p)\} & r = \frac{1}{5}s, \\ \{(0,q,1-q)\} & r = \frac{4}{3}s. \end{cases}$$

$$MBR_C(p,q) = \begin{cases} \{(1,0,0)\} & p > \frac{3}{8}q \text{ and } p > \frac{1}{5}q, \\ \{(0,1,0)\} & p < \frac{3}{8}q \text{ and } p < \frac{4}{3}q, \\ \{(0,0,1)\} & p < \frac{1}{5}q \text{ and } p > \frac{4}{3}q, \\ \{(r,1-r,0)\} & p = \frac{3}{8}q, \\ \{(r,0,1-r)\} & p = \frac{1}{5}q, \\ \{(0,s,1-s)\} & p = \frac{1}{5}q. \end{cases}$$

where p, q, r and $s \in [0, 1]$.
To compute the probabilities p, q, r and s corresponding to the players' mixed-straegies, we formulate the linear programs described in equations (3) and (4):

$$\begin{array}{ll} \text{Minimize} & x_1 + x_2 + x_3 \\ \text{Subject to} & 5x_1 - 3x_2 \geq 1, \\ & -x_1 + 4x_2 \geq 1, \\ & x_1 + x_2 + x_3 = \frac{1}{Z_V}, \\ & x_1 \geq 0,\ x_2 \geq 0, x_3 \geq 0. \end{array} \quad (3)$$

$$\begin{array}{ll} \text{Minimize} & y_1 + y_2 + y_3 \\ \text{Subject to} & 5y_1 - 3y_2 \geq 1, \\ & -y_1 + 4y_2 \geq 1, \\ & y_1 + y_2 + y_3 = \frac{1}{Z_C}, \\ & y_1 \geq 0,\ y_2 \geq 0, y_3 \geq 0, \end{array} \quad (4)$$

where:

- p, q, $u = 1 - p - q$, r, s and $t = 1 - r - s$ are respectively the probabilities of playing T_v, L_v, I_v, T_c, L_c and I_c.
- $W_1(p, q, u, T_c)$ is v's win if c plays T_c.
- $W_1(p, q, u, L_c)$ is v's win if c plays L_c.
- $W_1(p, q, u, I_c)$ is v's win if c plays I_c.
- $W_2(r, s, t, T_v)$ is c's win if v plays T_v.
- $W_2(r, s, t, L_v)$ is c's win if v plays L_v.
- $W_2(r, s, t, I_v)$ is c's win if v plays I_v.
- $Z_V =$ Minimize $(W_1(p, q, T_c),\ W_1(p, q, L_c),\ W_1(p, q, I_c)))$, $Z_V > 0$.
- $Z_C =$ Minimize $(W_2(r, s, T_v),\ W_2(r, s, L_v),\ W_2(r, s, I_v)))$, $Z_C > 0$.
- $x_1 = \frac{p}{Z_V}$, $x_2 = \frac{q}{Z_V}$ and $x_3 = \frac{u}{Z_V}$.
- $y_1 = \frac{r}{Z_C}$, $y_2 = \frac{s}{Z_C}$ and $y_3 = \frac{t}{Z_C}$.

Then, we use the *Simplex* algorithm to solve equations (3) and (4). The resolution leads to the following values: $p = \frac{7}{13}$, $q = \frac{6}{13}$, $u = 0$, $r = \frac{7}{13}$, $s = \frac{6}{13}$ and $t = 0$.

5 Results

At issue of the optimal results achieved by the *Simplex* resolution, we check Verifier and Claimant probabilities matching with the mutual best-responses' correspondence ($MBR_V(r, s)$ and $MBR_C(p, q)$) computed on the previous section. The Claimant probability $r = \frac{7}{13}$ corresponds to the case where T_v is the best-strategy for the Verifier. In fact, r is greater than $\frac{3}{8}s$ and than $\frac{1}{5}s$. Analogously, the Verifier probability $p = \frac{7}{13}$ yields to the case where T_c is the Claimant's best-strategy. In fact, p is greater than $\frac{3}{8}q$ and than $\frac{1}{5}q$. Thus, the mixed-strategy Nash equilibrium of our game corresponds to the situation where saying the truth and cooperating is the best-strategy for both players. Consequently, the best strategy for the Verifier is T_v and the best strategy for the Claimant is T_c and both players have no incentive to deviate from such situation. This means that according to our bidirectional authentication, the two Bluetooth devices in communication have better to be trusted.

6 Our bidirectional Bluetooth authentication protocol

Our method include two main phases: the authentication security parameters phase and the authentication game establishment phase. The first phase is used to define the devices trustworthiness and consequently the players' strategies. The second phase corresponds to our game-theoretic model where we consider the bidirectional authentication as a bimatrix game.

6.1 The security parameters check phase

According to the classical Bluetooth authentication (see figure 1), the Verifier and the Claimant devices use respectively theirs input parameters to produce the $SRES$ and ACO outputs. For both devices, there is only one secure parameter, the $BDDR\_C$ relative to the Claimant, and only the Verifier cheks if the two $SRES$ correspond. So, the Verifier can establish the trustworthiness or the untrustworthinessof its correspondent. Consequently, it can accept or refuse the communication without any risk. But, if the Verifier is a malicious device, the Claimant isn't able to discover it and the Verifier can easily damage its correspondent.

Consequently, in our bidirectionnal model, we consider additional input parameters. For both players' existent input parameters, we add $RAND(C)$ and $BDDR\_V$. Thus, the security parameters check phase include two main steps. First, the Verifier

check the Claimant identity. Next, the Claimant takes the role of the Verifier and check its correspondent identity. Note that this identity check is done during two differents sessions and isn't bidirectional. In each step, each device compute an output and then, the two devices check for correspondence. The Verifier and the Claimant compute, respectively, $SR1$ and $SR2$ in the first step, and $SR3$ and $SR4$ in the second step.

6.2 The authentication game phase

The authentication game phase consists in modeling the bidirectional Bluetooth authentication as a game between the Verifier and the Claimant. To define the players strategies, we use the results achieved in the first phase. In fact, the strategies taken by the devices are derived from the matching between the outputs. Thus, if $SR1 = SR2$ this means that the Claimant is trusted and ready to communicate. Else, the Claimant is considered as a malicious device trying to damage the Verifier. On the other hand, if the Claimant doesn't return a result, this means that it is indifferent to the communication. The same reasoning is used for the Verifier where, this time, the $SR3$ and $SR4$ results are used.

After deriving the players' strategies, we define our utility function parameters. These parameters represent the cost and reward functions coefficients affected to each player, depending on his strategy and the one of his correspondent. Next, we compute our Nash equilibrium (or best-responses correspondence) as detailed in section 5.3. Consequently, our Nash equilibrium represents a pair of strategies (one by device) where each player is saying the truth and wanting to securely communicate whith his correspondent. In a Nash equilibrium, no player has an incentive to deviate from his strategy (no device can get a higher gain when deviating from its Nash equilibrium strategy). In terms of Bluetooth security, our bidirectional authentication is successful if and only if both devices are trusted and there isn't any risk of damage or impersonation.

6.3 BiAuth algorithm

We summarize our bidirectionnal authentication procedure on an algorithm called BiAuth. The mains steps of our algorithm are described as follows:

Algorithm BiAuth

1. Security parameters check:
   (a) Define the authentication security parameters.
   (b) Compute the security parameters correspondences.
2. Authentication game:
   (a) Define the game basic elements:
      - Define the set of players (a Verifier device and a Claimant device).
      - Define the players' pure strategies (depending on security parameters check results).
      - Define the players' mixed strategies.
      - Define the players' utility functions.

   (b) Find mixed Nash equilibrium:
      - Compute Verifier and Claimant pure-strategy best-responses' correspondence.
      - Compute Verifier and Claimant mixed-strategy best-responses' correspondence.

   (c) Formulate Verifier and Claimant problems as linear programs.
   (d) Compute mixed strategies' probabilities: *Simplex* resolution.
   (e) Compute mixed Nash equilibrium.

Figure 2 illustrates our bidirectional Bluetooth authentication protocol where:

- RV and RC are randoms numbers generated, respectively, by the Verifier and the Claimant.
- BV and BC are, respectively, the Verifier and the Claimant Bluetooth addresses ($BDDR$).
- LK is the link key.
- ACO is the Authenticated Ciphering Offset generated by the authentication process.
- FV and FC are, respectively, the Verifier and the Claimant functions used to check their correspondent identity.
- $E1$ is the cryptographic function used during the unidirectional Bluetooth authentication.
- SSV and SSC are the set of all possible strategies for the Verifier and the Claimant, respectively.
- PRV and PRC are, respectively, probabilities about Verifier and Claimant strategies.
- UV and UC are, respectively, the Verifier and the Claimant utility functions.
- CNE_V and CNE_C are the functions used to compute the best-responses correspondence, respectively, for the Verifier and the Claimant.
- NEV and NEC are respectively, the Verifier and the Claimant Nash strategies.

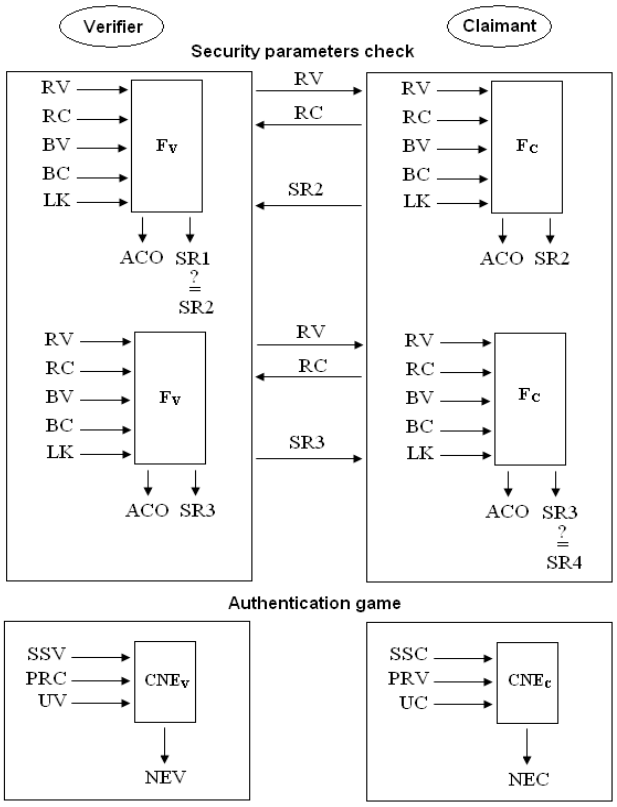

Figure 2: Our bidirectional Bluetooth authentication protocol.

6.4 Attacks scenarios

As previously cited, an important risk incurred in the classical Bluetooth authentication is linked to a malicious Verifier. Such device can attack a trusted Claimant by nasty messages and damage it. According to our authentication model, such scenario won't be able to occur. In fact, when considering our game, the strategies pairs (Lie and try to damage the Claimant, Say the truth and communicate with the Verifier) don't represent a Nash equilibrium. Another possible attack is the Man-in-the-Middle attack where an attacker device inserts himself "in between" two Bluetooth devices. The attacker connects to both devices and pretends to each of them to be the other device. Our bidirectional authentication can prevent such attack. Indeed, the attacker couldn't impersonate any device in communication. The attacker must authenticate itself as a trusted device for each Bluetooth device. Else, the authentication fails.

Conclusion and perspectives

In this work, we presented a solution to strengthen the Bluetooth security. A classical Bluetooth authentication is unidirectional and consequently is vulnerable to malicious device attacks. Our idea was to propose a bidirectional authentication scheme. We were interested in game theory because it gives a framework to formally respresent many real-life problems. Thus, we viewed the authentication between two Bluetooth devices as a game. We modeled our bidirectional authentication as a two-player simultaneous game (bimatrix), we defined the possible strategies for each player (based on some security paremeters check) and we formulated our utility function. Such function affects some costs and rewards values for each player depending on his strategy and the one of his correspondent. Then, we computed the best-strategies for each player (defining the Nash equilibrium) and defined players' total gains by linear programs (solved by *Simplex* algorithm). We finded only one Nash equilibrium corresponding to the case where both players are saying the truth. In Bluetooth security terms, two devices have better to be trusted during our bidirectional authentication. In other words, our authentication is successful if and only if both devices are authentic.

To implement our protocol, two issues are possible: outside the Bluetooth core protocol (in the application layer) and within the Bluetooth core protocol (in the LMP layer). In the first case, the classical Bluetooth authentication will be replaced by our bidirectional authentication. When considering the second view, we have to add some changes in the cryptographic function used during a classical Bluetooth authentication in order to incorporate our model. We are finalizing some benchmark to compare the efficiency between our algorithm and the standard Bluetooth authentication model.

Our work can be extended of different manners. We can model our bidirectional authentication as an N-player game. According to such model, an authentication process can be performed between many devices at the same time. This will be useful when *piconets* or *scatternets* are formed. In addition, we can represent our model in extensive form and consider it as repeated game to describe the dynamic behavior. A player will take into account the effect of his current behavior on the other players' future behavior. This principle can forewarn trusted Bluetooth devices of possible threats and malicious devices. In

other hands, our model can be applied to any authentication process. The only changes to introduce concern the utility function parameters.

References

[1] Alexoudi, M., Finlayson, E., & Griffiths, M. (2002). *Security in Bluetooth.*

[2] Bray, J., & Sturman, C. F. (2002). *Bluetooth 1.1: connect without cables.* Second Edition, Prentice Hall PTR (Eds.).

[3] Browne, R. (2000). *C4i defensive infrastructure for survivability against multi-mode attacks.* In Proc. 21st Century Military Communications - Architectures and Technologies for Information Superiority.

[4] Buike, D. (1999). *Towards a game theory model of information warfare.* Master's Thesis, Technical report, Airforce Institute of Technology.

[5] Candolin, C. (2000). *Security Issues for Wearable Computing and Bluetooth Technology.* Telecommunications Software and Multimedia Laboratory, Helsinky University of Technology, Finland.

[6] Cordeiro, C. M., Abhyankar, S., & Agrawal, D. P. (2004). *An enhanced and energy efficient communication architecture for Bluetooth wireless PANs.* Elsevier.

[7] De Kock, A. *Bluetooth security.* University Of Cape Town, Department Of Computer Science, Network Security.

[8] Del Vecchio, D., & El Kadhi, N. (2004). *Bluetooth Security Challenges, A tutorial.* In proceedings of the 8th World Multi-Conference on Systemics, Cybernetics and Informatics, Orlando, Florida, USA.

[9] Kitsos, P., Sklavos, N., Papadomanolakis, K., & Koufopavlou, O. (2003) *Hardware Implementation of Bluetooth Security.* IEEE CS and IEEE Communications Society, IEEE Pervasive Computing.

[10] Muller, T. (1999). *Bluetooth security architecture - Version 1.0.* Bluetooth white paper.

[11] Osborne, M.-J., & Rubinstein, A. (1994). *A course in game theory.* Massachusetts Institute of Technology.

[12] Persson, J., & Smeets, B. (2000). *Bluetooth security - An overview.* Ericsson Mobile Communications AB, Ericsson Research, Information Security Technical Report, Vol 5, No. 3, pp. 32-43.

[13] Pnematicatos, G. (2004). *Network and Inter-Network Security: Bluetooth Security.*

[14] Syverson, P. F. (1997). *A different look at secure distributed computation.* In Proc. 10th IEEE Computer Security Foundations Workshop.

[15] (2003) *Bluetooth: threats and security measures.* Bundesant fr Sicherheit in der Informationstechnik, Local Wireless Communication project team, Germany.