Bluespam Filtering

Mihai DOINEA, Madalina ZURINI
Academy of Economic Studies, Bucharest, Romania
mihai.doinea@ie.ase.ro, madalina.zurini@gmail.com

The paper whishes to present the importance of protecting mobile phones from unwanted or illegal messages received via Bluetooth communication channel. The Bluetooth technology is highlighted. Security dimensions for Bluetooth communication are presented and ways of analyzing and classifying spam messages are discussed. A BMFA, Bluetooth Message Filter Architecture is proposed for further implementation.
***Keywords**: Security, Spam Filtering, Bluetooth Messages, Bayesian Analysis, Mobile Devices*

1 Bluetooth Technology

Along with the progress of mobile communication and the development of multimedia technology, a new branch has emerged, requesting the necessity of multimedia content transmission. For this purpose, in a first stage, infrared communication was implemented for helping users change digital content between mobile devices. **I**nfra**r**ed **D**ata **A**ssociation or IrDA developed the infrared standards which allowed users to change files using infrared light on short distances with the following characteristics found in today's specifications:

- 4 to 10 times faster than the first IrDA protocols used;
- up to 3 meters in length the distance between devices;
- speeds up to 1 Gbit/s compared with the lowest rate of 9600 bit/s, used in PDA communications formats such as HPSIR and ASKIR.

But IrDA popularity dropped when the new millennium came with other wireless technologies such as WiFi and Bluetooth which overlapped the obstacles given by the use of IrDA, for the following reasons:

- they don't need a direct line of sight between the receiver and transmitter;
- have speeds greater than the ones provided by infrared technology;
- they are suited for lots of implementations where wireless connections are necessary.

Bluetooth is a short range wireless technology which is growing rapidly, as the number of Bluetooth chips released on the market per year is increasing almost exponentially. As presented in [1] Bluetooth is operating in the **I**ndustrial, **S**cientific and **M**edical band, ISM at 2.4 GHz with typical average ranges fluctuating around 100 m for class 1 devices, around 10 meters for class 2 devices, and around couple of meters for class 3 devices. Due to the fact that Bluetooth technology is using radio waves for transmitting data, the protocol had to develop tolerance mechanisms to overlap such problems.

The speeds of Bluetooth communication have grown from the first version with speeds around 1 Mbit/s up to 24 Mbit/s for version 3.0 and even more for version 4, comparable with mobile phone technology.

The basic Bluetooth network topology is called *piconet*. A piconet network is a **W**ireless **P**ersonal **A**rea **N**etwork, WPAN in which two or more devices are synchronized to a common clock. When two or more devices connect to each other in a Bluetooth connection than protocols specially designed for this type of link are handling all the aspects of the communication process starting from the initialization stage, the management of the connection and ending with the stage of closing and releasing the resources used for the link. In a Bluetooth connection, one of the devices which are part of it is called slave and the other one is called the master.

The piconet architecture as presented in [1], [2] can handle no more than seven active devices in role of a slave of which

frequencies are determined by the master who is managing them. So in this way two slaves can't communicate each other independently of the master.
Using a technique called time division, Bluetooth devices could participate simultaneously to several piconets, forming a new topology called scatternet, an adhoc network of Bluetooth devices formed from overlapped piconets.
In [1] it is mentioned that a Bluetooth device can simultaneously be slave in different piconets networks or master in one and slave in another but never master in two or more piconets because the frequencies of the slaves are dictated by the master address and its clock value meaning that those piconets are in fact just one, as depicted in figure 1.

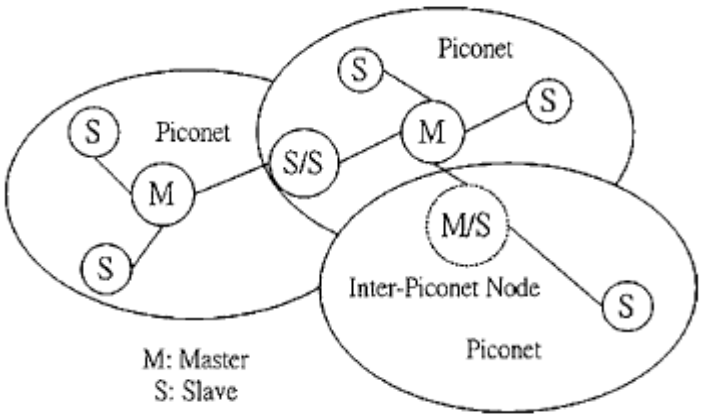

Fig. 1. Piconet nodes in a scaternet network

Besides these existing topologies, Bluetooth can be used to provide network access by using the Bluetooth-IP services and effectively enlarging the possibilities of changing large amounts of information as if we do it in a usual IP network.
In [2] is described how Bluetooth can access IP networks services by using the Point-to-Point Protocol, PPP and the Bluetooth Network Encapsulation Protocol, BNEP, helping devices to map IP addresses with the corresponding Bluetooth addresses.
Like Harold Osborne predicted on the middle of XIX century, the mobile devices and their power of communication will lead humanity to a period when every born child will be given a small device on which all important information will be held, like the unique identification number, social insurance, address, etc. and no one will be in need of other kind of support for keeping their personal information [3].

2 Security dimensions

As more and more people are willing and actually do use the mobile communication devices, laptops, digital cameras and other multimedia devices, the need for ergonomic things, more compact and easy to manage is increasing and dictates the leadership on such kind of markets.
The fact that Bluetooth technology is easy to operate makes the devices which implements it widely accepted because:

- no need of cables for connecting two or more devices;
- the easiness of connecting devices without any setup knowledge for the connection;
- a wide range of utilization of this technology.

Having this said, we can further explore the great opportunities brought by this technology, but also we must not omit all the drawbacks and vulnerabilities to which we are exposed when actually we are using it on large scale, which is the case of today's time.
In Western Europe and also in North America, a very large percent of mobile devices have implemented Bluetooth microchips, as a recent study is showing in [4]. Over 70 percent in Europe and more than 60 in North America of mobile phones released on the market have BT microchip.

Deep analyses were made upon how Bluetooth is used when it is about marketing. In [4] it is showed that youth is a major factor which influences how BT is accepted and used as a mean of advertising.

Although the use of mobile devices in daily life is increasing in the developed countries, the acceptance of mobile advertising is not implicitly deduced, as a large majority of people tend to take this is a bluespam.

Security good points for Bluetooth technology lies in the following characteristics:

- the ability of adaptive frequency hopping, in this way limiting interferences from other frequencies;
- encryption extensions for different aspects of communication;
- PIN code authentication capability, for allowing other devices to connect;
- Quality of Service control.

Negative security aspects of Bluetooth technology consists in:

- theft of information by hacking into device without passwords or left unprotected;
- Denial of Service attacks against Bluetooth devices;
- remotely execution of malicious code using a Bluetooth connection;
- airborne viruses or worms received through backdoors left open in the BT protocol;
- capability of using social engineering to get access to BT devices.

The capability of malicious users to actually damage a system by using the Bluetooth protocol interface for connecting to it, is relatively small. Viruses or worms sent through a BT connection are slowly spreading since the possible targets of infection are determined by the user mobility. A high rate of success is by using the second door through which they can penetrate the system, the MMS service. In this way, threats can easily read the phone agenda and multiply by sending MMSs around the world in just couple of seconds as presented in [5].

Another important aspect of BT security is determined by the marketing directions to Bluetooth enabled device usage for sending unsolicited commercial material. Unsolicited communication, no matter via which means is conducted, is considered to be an intrusion act to the privacy of users. In this framework, Bluetooth enabled devices could be bombed with commercial material until saturation or even, if by mistake we accepted it, can inflict important damage to our devices.

The existing legislation defines what is called unsolicited commercial communication and direct marketing but it was only made when the technology was full with electronic mails, SMSs and other kind of means of publicity. Since the Bluetooth enabled devices, the legislation partially changed to include this kind of publicity also, but nonetheless it is still uncertain about the way how bluespams must be classified.

According to [6] the legislation analyze if an electronic delivered message came without the prior user request, based on the following criteria:

- if the action of sending the message is an electronic communications service;
- whether this service is offered using a communication network;
- whether the aforementioned service and network are public.

In [6] it is argued that based on the aforementioned criteria, messages delivered by Bluetooth enabled devices can't be covered by the anti-spam legislation, nor they can be treated like a legitimate message which users prior solicited.

Nonetheless, with or without the legislation for Bluetooth messages, they are seen like intruders in the consumer's privacy, taking because of that the name of bluespam.

3 Spam analysis

Spam messages are an increasing threat to mobile communication because of the decreasing of the text costs. In [8] is presented the fact that these trends have attracted a large number of phishing and spamming attacks using phone messages. The decision that must be taken in consideration is the type of messages that a mobile owner receives over the phone.

Classification of mobile text messages leads to analyzing the appearance of basic units that are represented by the words from which the message body is composed. There are several types of classification but the one developed in this paper for the proposed architecture is the supervised Bayesian classification that can predict class memberships.

Breaking the message *M* in words implies considering that the probability of the message is equal to the probability of the combined words:

$$P(M) = P(w_1, w_2, \ldots, w_m)$$

In order to calculate the value of $P(w_1, w_2, \ldots, w_m)$ we need a huge dataset that contains all the possible combinations of the words that are required to calculate our message probabilities. The first assumption that this classification is based on is the fact that the words in the messages are independent of each other and randomly displayed in the message, like in [9].

Thomas Bayes is the English mathematician that formulated the theory that is called after him, theory that takes in the center the notion of probability as being something partially known, not as a frequency.

Having the probabilities and the events as the nodes, the Bayesian network appears as a graphic model that represents the probabilistic relations between the values of the events which are a part of the events proposed for analysis, in other words, a directed acyclic graph, DAG, as it is seen in [10].

In the last period, the Bayesian networks had become a frequently used method for presenting uncertain knowledge and the influences that exists inside of it. This technique brings advantages such as:

- handling incomplete date sets – Bayesian classification models can produce predictions with high accuracy on the explanatory variables of regression models;
- ease of detecting the existence of casual relations – Bayesian networks return weights that explains the dependence between different factors of influence analyzed, in addition helping to a good explanation of the processes' variables of different complexity;
- combining knowledge with data – these networks allow prior data integration because of the property held of being casual semantic.

Bayesian probability, as seen by Thomas Bayes and later by other researchers, is different from probability seen in the classic sense. While classical probability refers to the physical properties of the world seen in terms of general, Bayesian probability brings the spotlight to pursue the principle of future events.

Introducing the human factor in the equation, the field of probability theory has been questioned whether or not the new system could be applied within the Bayesian networks. The reference axiomatic system of these probabilities is the Kolmogorov system, namely:

Axiom 1 (Nonnegative). For each random event from the field of events named an attached a nonnegative real number P (E) called the probability of E.

Axiom 2 (Normality). The probability of the total event P (T) = 1.

Axiom 3 (Extended additive). If the occurrence of an event E is equivalent to the appearance of a certain event E_1, E_2, ..., E_n, ..., two by two incompatible, then P (E) = P (E1) + P (E2) + ... + P (En) + ...

To the graphical representation of the Bayesian networks the Bayes theory is added, defined as the following:

$$P(H/D) = \frac{P(D/H) * P(H)}{P(D)}$$

where:

- H – hypothesis and D – dates;
- $P(H)$ – the prior probability of H, the probability that H is true, before the dates D to be seen;
- $P(D/H)$ – the conditioned probability being given the D dates and the H hypothesis accomplished;
- $P(D)$ – the realization probability of D

dates;

- $P(H/D)$ – the probability of H hypothesis to be realized, being given the D dates and having information regarding the prior presumption upon the hypothesis.

Applying the Bayes theorem assumes a knowledge base to characterize a priori input. To solve the classification, the next four steps are followed:

- populating the knowledge base;
- calculation of Bayesian probability;
- aggregation of the probabilities;
- interpretation of the results.

Based on the filtering proposed in [11], populating the knowledge base for the bluespam classification involves decomposing the text messages to the base unit, the words, and counting the appearance of each word in the ham and spam messages. The decomposing is done using token separators over the body of the message, tokens such as: {‘,’, ‘.’, ‘!’, ‘?’, ‘(’, ‘)’}.

Having formed the knowledge base, the next step can be processed using the following formula for each word of the message *M:*

$$P(S/W) = \frac{P(W/S)}{P(W/T)}$$

where:

- $P(S/W)$ – the probability of the message that contains the word *W* to be spam;
- $P(W/S)$ – the probability of appearance of the word *W* in all the spam messages;
- $P(W/T)$ – the probability of appearance of the word *W* in all the knowledge base messages;
- $T = S + H$ – the total messages of the knowledge base.

Aggregation of the probabilities is achieved by extending the conditional probability formula to the entire set of words that makes up the message that represents the input data for the classification.

The emergences of the *m* words of the M message are considered to be independent events and the aggregation can be applied:

$$P(SPAM/M) = P(S/W_1) \bullet P(S/W_2) \bullet P(S/W_3) \bullet \cdots \bullet P(S/W_m) = \prod_{i=1}^{m} P(S/W_i)$$

where:

- $P(SPAM/M)$ – the probability of the message *M* to be spam;
- $P(S/Wi)$ – the probability of the message that contained the word W_i to be spam.

For the ham probability $P(HAM/M)$, the aggregation used is:

$$P(HAM/M) = \prod_{i=1}^{m} P(H/Wi)$$

where:

- $P(H/Wi)$ – the probability of the message that contained the word W_i to be ham.

The interpretation of the results is based on the two probabilities $P(HAM/M)$ and $P(SPAM/M)$ as follows:

- if $P(SPAM/M) > P(HAM/M)$, then message *M* is considered to be a spam one;
- if $P(SPAM/M) <= P(HAM/M)$, then message *M* is considered to be of ham type.

Must be mentioned that, in case of bad classification, as in the interpretation of the results, two types of errors can occur, the false positives and the false negatives. A false positive message is an innocent spam message that gets mistakenly identified as ham, while a false negative is a message that is ham but the classifier interprets it as being spam.

The Bayesian spam filtering has two major objectives, to reduce the false negatives and positives. For that, for the Bayesian function, let it be called the *F* function, the following set of conditions must be met:

$$(Conditions): \begin{cases} F: M \rightarrow \{0,1\} \\ \min_{false\ positives} F \\ \min_{false\ negatives} F \end{cases}$$

- *M* – the lot of classified messages, where $M = M_1 \cup M_2 \cup M_3 \cup \cdots \cup M_m$, considering a set of *m* messages that have been classified with the Bayesian filtering;

- *{0,1}* – are the two values that the *F* function returns, 0 for ham and 1 for spam.

Not the rate of false positives worries or should worry a user, but the rate of false negatives. In order to fight with those two fakes, the Bayesian classifier is trained with a double rate for the ham messages, therefore to a ham message is assigned a double appearance for strengthening the probability of that word to be ham, in terms of spam filtering, the word is called hammier.

Because of the fact that spam filtering is a race between spammers and spam filtering developers, the different implementations of this type of classification will never stop as long as new techniques of spam aspects will still appear in our daily activities, from the email inbox to the messages received over the phone.

4 Filtering architecture

In our days, decision is the activity that consumes more and more time and material resources, being defined as the conscious activity of choosing an acting method from a range of alternative for realizing the proposed objectives. Decision being part of the management functions can lead us to the idea that a mobile message classification is a decision process from the mobile management field that improves the time spent for handling unwanted messages received on the phone.

For this reason this paper proposes a BMFA, Bluetooth Message Filter Architecture which has as main objective the classification of unsolicited BT text messages in bluespam or blueham.

When a BT advertising message is received, if there wasn't any prior authentication between the transmitter and receiver, a message pops-up asking user if he wants to accept the incoming connection. This is the first step in which unsolicited messages can be rejected, but there's no way, at a first look, of telling whether the message is from a reliable source or not. So we are in the position of choosing between:

- whether accept the incoming connection and with it all the possible unwanted events if the message came indeed from a harmful target;
- whether reject it and maybe lose something of interest that had no intention of jeopardize the security of our BT device.

But messages could be received also without any prior notification of the intention of sending it. In this case, the presented BMFArchitecture, figure 2, is wanted to bring some protection by classifying the Bluetooth text messages received in this way or filtering the unknown messages accepted for being received.

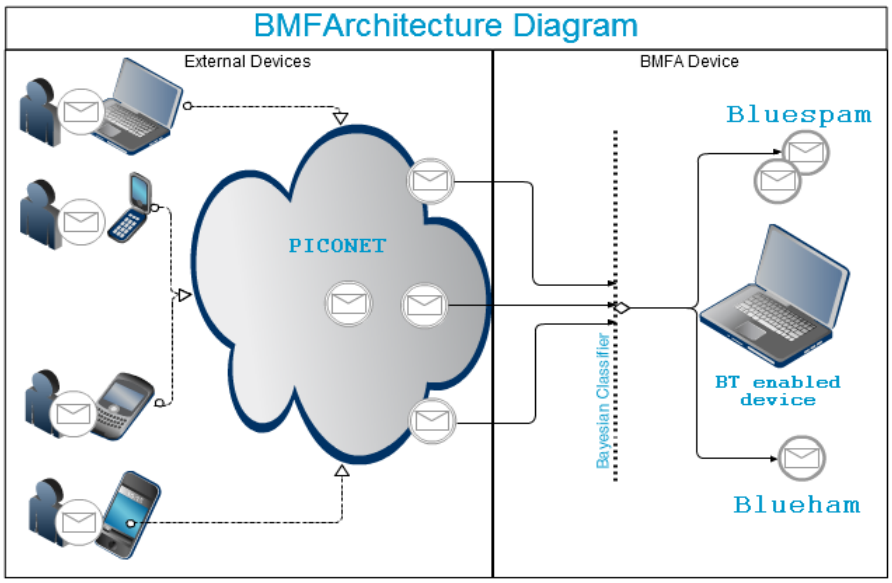

Fig. 2. BMFArchitecture Diagram

After messages have left the sender they are managed according to the piconet architecture schema for being delivered to the recipient. Once they reached destination, they will enter into the Bayesian Classification diagram depicted in figure 3. From here the BT text messages will end up into one of the two categories to which the Bayesian Classifier is throwing the results: bluespams or bluehams.

Figure 3 contains the four steps presented for the Bayesian classification in a logic diagram.

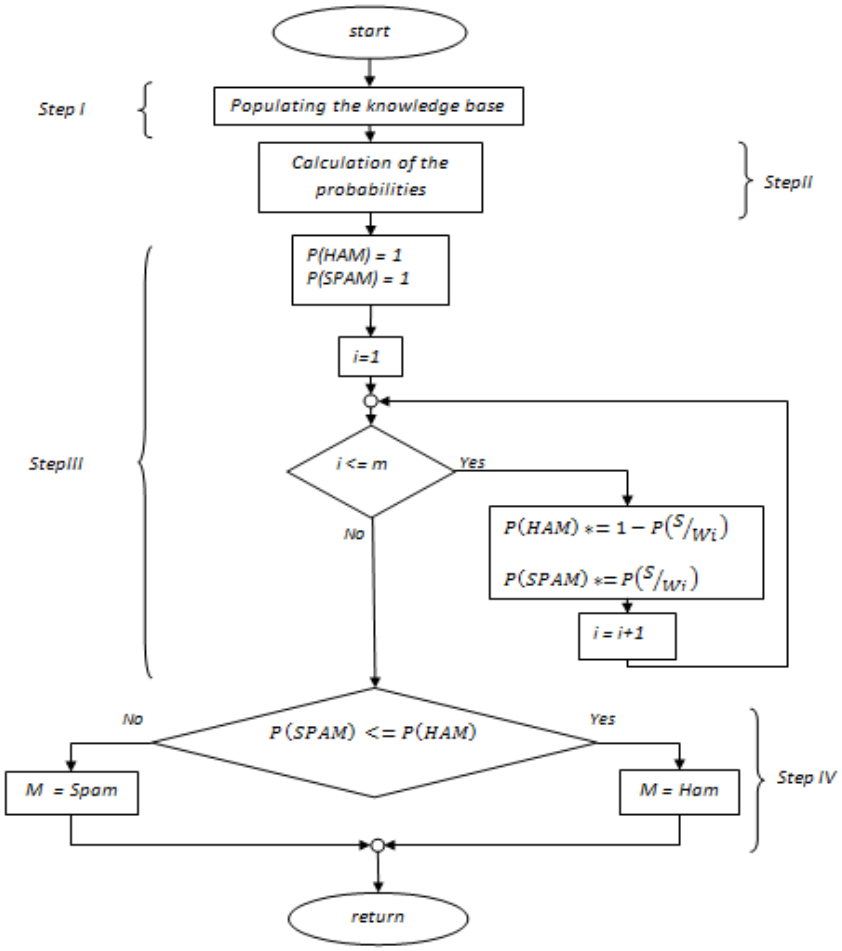

Fig. 3. Logic diagram of the Bayesian classification

For using every word which is part of the message analyzed, implies having a probability for it already defined in the knowledge base. But what happens when a new word is part of our message? For those unknown tokens a different point of view must be taken into consideration. Paul Graham, in his spam filter described in [11], used a fixed probability for this kind of words, 0.4, implying that the new word is more ham, than spam. Other researchers used varieties of values, values that are directed to the particularities of the messages' owner. In our classification, we consider that the new tokens have the probability equals to the probability of a message to be spam from the total base of messages used for the training.

For processing the BT messages, an indexed data file will be used for faster access to the records. The classification process will be entirely run on the BT device, but the training process could even be ran on devices which have higher computational power and then the result transferred back to the BT device.

5 Implementation's results

The process of verification and validation

aims to characterize the quality of the implementation, implying a second goal that is to discover the inconsistency with the requirements presented in the stage of the defining of the problem, detailed in [12]. Using a dynamic validation, a vector of input data is created, called the data testing, afterwards the desired results are compared with the one resulting in the execution.

Let $O : \mathcal{M} \rightarrow \mathbf{R}$, where $O(x) = \frac{NMN}{TC}$ and:

- NMN – the number of mobile messages correspondently classified;
- TC – the medium time of classification of a mobile message;
- $\mathcal{M}$ - the total number of mobile messages used in the system.

Optimizing the function *O(x)* in terms of maximization can be made by following simultaneously the following objectives*:*

- maximizing *NMN*;
- minimizing *TC*.

The component *NMN* is analyzed from the functionality quality characteristic point of view, meaning the behavior of a software product to realize its proposed objective. For a better representation of the results, NMN in transformed into $I_{NMN} \in [0,1]$., the indicator of the number of mobile messages correspondently classified equal to:

$I_{NMN} = \frac{NMN}{\mathcal{M}}$, with:

For demonstrating the utility of the Bayesian classification algorithm, BMF, a series of trainings and classifications were made within [13]. Using the least square method on 200 mobile messages for estimating the linear dependency between total time of classification and the number of classified messages, the following equation was established, also presented graphically in figure 4:

$$time = 12.4703 + 1.5005 * nrmail,$$

where:

- *time* – the endogenous variable, dependable on the exogenous variable *nrmail;*
- *TC* – the medium time of classification of a message and is equal to $\frac{\partial time}{\partial nrmail}$ = 1.5005 seconds/ message.

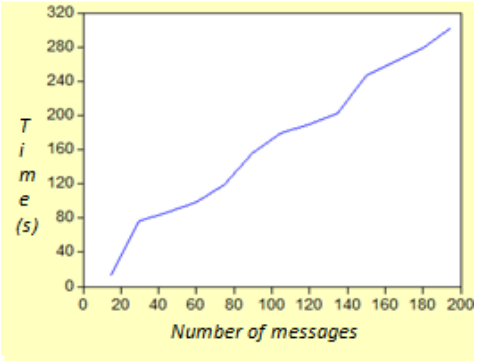

Fig. 4. TC evolution

In the mean time, the degree of correct classification I_{NMN}, was counted using an estimation function, *f(x),* of the Bayesian classification. Being a supervised algorithm, a learning function *f(x)* is associated to the Bayesian filtering, as presented in figure 5:

$$f(x) = y, and \begin{cases} x - time \\ y - threshold\ of\ good\ classification \\ \lim_{x \to \infty} f(x) = 1 \end{cases}$$

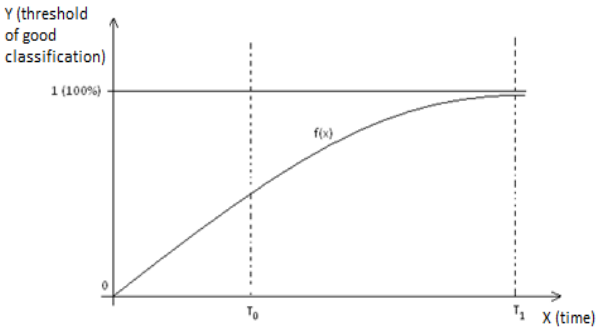

Fig. 5. Bayesian learning function

For our 200 messages used for training the learning function, the results indicated a degree of 99%, $I_{NMN} = 0.99$, with only 2 wrong classifications from the total of $Card_M$ = 200.

As for the time evolution that implies a larger set of training messages, the learning function will tend more to the threshold value of 1 (100%), meaning that more messages will be correct classified as the set of messages is greater.

6 Conclusions

The new emerged technologies forced in the same way, end-users and attackers, to find new methods of adapting their needs. This great dynamicity is in fact an advantage for the end-users who can enjoy the benefits of the new technology in a short time window, until attackers will learn how to exploit it.

Unfortunately, Bluetooth technology isn't yet well settled, having major drawbacks on the authentication protocol and other backdoor vulnerabilities. But either way, we think that the advantages brought by this novel wireless technique of communication are far above the threats which can reduce the enthusiasm of actually using it, as an old quote is saying: "*To win you have to risk loss*", by Jean-Claude Killy.

Even though there are holes because of the Bluetooth security aspects, applying a simple statistic filtering method, such as the naive Bayes classification which is known to have a high performance in achieving the desired aims, can cover those drawbacks in order to maintain a secure level for the benefits of the end-users.

Acknowledgements

This article is a result of the project „Doctoral Programme and PhD Students in the education research and innovation triangle". This project is co funded by European Social Fund through The Sectorial Operational Program for Human Resources Development 2007-2013, coordinated by The Bucharest Academy of Economic Studies (project no. 7832, "Doctoral Programme and PhD Students in the education research and innovation triangle, DOCECI").

References

[1] A. Hernandez, I. Alastruey and A. Valdovinos, "Network architecture planning and handoff strategies enabling QoS-aware bluetooth based networks with full mobility", *IEEE Transactions on Consumer Electronics*, Vol. 54, No. 3, pp. 1130-1138, 2008.

[2] W.C. Chan, J.L. Chen, P.T. Lin and K.C. Yen, "Quality-of-Service in IP Services over Bluetooth Ad-Hoc Networks", *Mobile Networks and Applications*, vol. 8, No. 6, pp. 699-709, 2003.

[3] R. Ling, *The mobile connection: the cell phone's impact on society*. USA: Elsevier Printing House, 2004.

[4] S. Leek and G. Christodoulides, "Next Generation Mobile Marketing: How young consumers react to Bluetooth enabled advertising", *Journal of Advertising Research*, Vol. 49, No. 1, pp. 44-53, 2009.

[5] S. Havlin, "Phone Infections", *Science Magazine*, Vol. 324, No. 5930, pp. 1023-1024, 2009.

[6] E. Kosta, P. Valcke and D. Stevens, "Spam, spam, spam, spam … Lovely spam! Why is Bluespam different?", *International Review of Law, Computers & Technology*, Vol. 23, No. 1-2, pp. 89-97, 2009.

[7] S. Jung, A. Chang and M. Gerla, "New bluetooth interconnection methods: Overlaid Bluetooth Piconets (OBP) and Temporary Scatternets (TS)", *Computer Communications*, Vol. 30, No. 10, pp. 2258-2273, 2007.

[8] J. W. Yoon, K. Hyoungshick and J.H. Huh, "Hybrid spam filtering for mobile communication," *Computers & Security*, Vol. 29, No. 4, pp. 446-459, 2010.

[9] T. Sun, "Spam Filtering based on Naïve Bayes Classification", *in Communicating Mathematics*, Durham University, Department of Mathematics, 44 pg., 2009

[10] J. Chieng, R. Greiner, J. Kelly, D. Bell and W. Liu, "Learning Bayesian networks from data: an information – theory based approach", *Artificial Intelligence*, Vol. 137, No. 1-2, pp. 43-90, 2002.

[11] P. Graham (2002, August) A plan for Spam. *Paul Graham Website* [Online]. Available at: http://www.paulgraham.com/spam.html

[12] F. Ricca and P. Tonella, "Analysis and Testing of Web Applications", *in Proc. International Conference on Software Engineering*, 2001, pg. 25-34.

[13] M. Zurini, "Spam detecting using probability and Bayesian analysis", *M.S. thesis*, Academy of Economic Studies, Bucharest, Romania, 2010

Mihai DOINEA is a PhD candidate at the Academy of Economic Studies in the field of Economic Informatics. Part of his PhD was made as a young researcher at Amsterdam Business School. He has a master diploma in Informatics Security (2006) and he is also a lecturer assistant teaching data structures and advanced programming languages at the Academy of Economic Studies. He published more than 30 articles in collaboration or as single author and contributed to the publication of two books. His research interests are given as follows: informatics security, distributed applications, optimization criteria, databases, artificial intelligence, information management, security policies, mobile devices, networking and wireless communication.

Mădălina ZURINI is currently a PhD candidate in the field of Economic Informatics. She graduated the Faculty of Cybernetics, Statistics and Economic Informatics in 2008 and a master in computer science researching the *implications of Bayesian classifications for optimizing spam filters* in 2010. She is also engaged in Pedagogical Program as part of the Department of Pedagogical Studies. Her fields of interest are data classification, artificial intelligence, algorithm analysis and optimizations. She wants to pursue a pedagogical career.