Fuzzy Logic in Location-based Authentication

David Jaros, Zdenka Kuchtova, Radek Kuchta, Jaroslav Kadlec
Dept. of Microelectronics, FEEC
Brno University of Technology
Brno, Czech Republic
email: jarosd@feec.vutbr.cz, xkucht06@stud.feec.vutbr.cz, kuchtar|kadlecja@feec.vutbr.cz

***Abstract* - The article is focused on the possibility of using fuzzy logic principles in the authentication process in a computer network environment. Fuzzy logic could play an important role in authentication techniques where the input data is unclear or inaccurate and, therefore, the result of the process will also become unclear. Examples of this can be found in processing positional information concerning the user's location at a particular moment within the authentication process. The paper shows a possible solution to these difficulties by using a location-based authentication system which relates to the user's biometric data.**

Keywords - fuzzy logic; authentication; location; biometric data

I. INTRODUCTION

The article deals with the possibility of the usage of fuzzy logic in the authentication process and especially in location-based authentication. Currently electronic systems make decisions exclusively by using bivalent values when they perform an authentication. The more native approach could be by using a value within a continuous interval. One of the sources where fuzzy logic was used is detailed in [1]; this is focused on password security enhancement.

Let us imagine a specific situation: two people talk to each other, the first of them declares something to the second. The second person has to make a decision whether s/he will believe this declaration or not. The decision will not happen with absolute certainty.

Another aspect of the authentication process is the position of the authenticated user. The number of mobile devices such as laptops, smartphones and tablets continues to grow. The question "Where are you?" in the mobile environment is being asked more and more frequently. This is where fuzzy logic could be exploited with regard to location-based authentication, and in the authentication process generally. This will have the result that the user will be allowed access to protected services dependent on his/her position and on his/her trust level. This could be achieved by the use of several methods, for example; assessing the age of the provided position information and its accuracy.

In this article we will introduce the methodology of how to use fuzzy logic principles in the authentication system. The rest of the article is organized as follows. In Section 2 fuzzy logic is introduced and an overview is given concerning what is required for its usage in authentication systems. Section 3 will discuss the possibilities of how to get the user's positional information and how to transfer it through a chain form, from user to authenticator. Section 4 will show an example of an authentication system and an authentication terminal designed for location-based authentication. Section 5 is concerned with future work and issues that have to be taken into account.

II. FUZZY LOGIC FUNDAMENTALS

Fuzzy logic is an extension of set theory and logic operators [2].

In comparison with classic set theory the main difference is membership of an element to the set. In classic set theory an element is a member of a set or not, no other option is possible. In fuzzy logic theory an element is mapped to a fuzzy set by usage of a membership function. The difference is described in (1).

$$\mu_K: X \to \{0,1\} \mu_F: X \to [0;1], \quad (1)$$

, where μ_K is a membership function of classic set and maps elements to universe set X into two member set {0,1}. and μ_F is a membership function of fuzzy set and maps elements from universe set into values in the range from 0 to 1. This relation is depicted in the Figure 1.

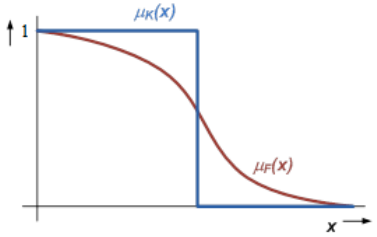

Figure 1. Fuzzy set membership function example

In fuzzy logic, we can talk about a "linguistic variable". When we consider a variable, in general, it takes numbers as its value. If the variable takes linguistic terms, it is called a "linguistic variable". Let us imagine the next example. We have a variable *X* called password strength, which has values (terms) *weak* ($\mu_N(n)$), *moderate*($\mu_S(n)$) and *secure* ($\mu_B(n)$). We can define the member function for each term as follows.

 ISBN: 978-1-61208-399-5

$$\mu_N(n) = \begin{cases} 1, for\ n \in <0;1>;\ n \in Z^+ \\ \frac{3-n}{2}, for\ n \in (1;3>;\ n \in Z^+ \\ 0\ for\ n > 3;\ n \in Z^+ \end{cases} \quad (2)$$

$$\mu_s(n) = \begin{cases} 0, for\ n < 2 \vee n > 6;\ n \in Z^+ \\ \frac{n-2}{2}, for\ n \in <2;4>;\ n \in Z^+ \\ \frac{6-n}{2}, for\ n < 4;6>;\ n \in Z^+ \end{cases} \quad (3)$$

$$\mu_B(n) = \begin{cases} 0, for\ n < 5;\ n \in Z^+ \\ \frac{n-5}{2}, for\ n \in <5;7>;\ n \in Z^+ \\ 1, for\ n > 7;\ n \in Z^+ \end{cases} \quad (4)$$

The equations stated above are displayed in Figure 2.

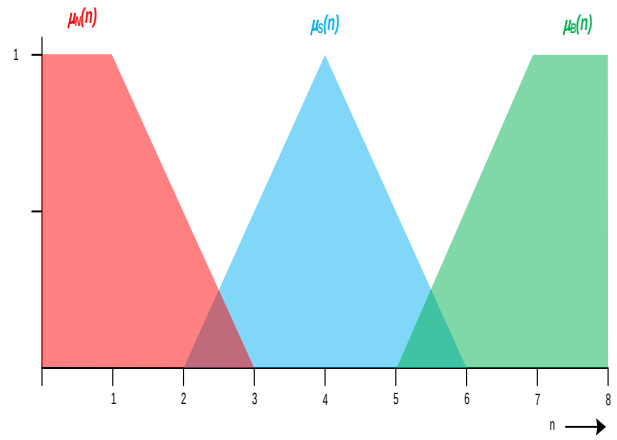

Figure 2. Password strength fuzzyfication

The fuzzy system is composed of input variables, output variables and inference rules. The inference rules are responsible for behavior of the system. Generally the rule is written in the form:

If*(ascendant)* ***then*** *(consequent),*

where the *ascendant* is one or more logically connected input variables and *consequent* is the output variable. Usually a system consists of a set of rules most of the time in several stages.

The logical connection of variables could represent Mamdani's implication, which could be explained by the equation 5 and Figure 3.

$$\mu_{\tilde{3}}(x_1, x_2) = \min\{\mu_A(x_1), \mu_B(x_2)\} \quad (5)$$

With regards to (6) the membership function of consequent will be cropped on layer equals to a minimum of values for both ascendant *min(α,β)*. The situation is illustrated in the figure 3.

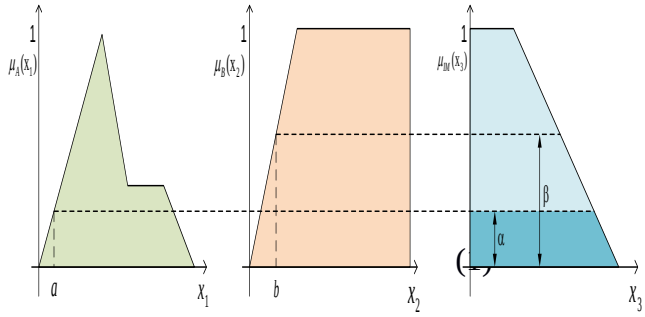

Figure 3. Mamdani's fuzzy implication

In this case we need to get a numerical value of the output linguistic value of the defuzzyfication to be done. Several solutions are possible for this task. In our case we will use the strategy: Center of Area (COA).

The widely used COA strategy generates the center of gravity of the possibility distribution of a fuzzy set (6).

$$x_{OUT} = \frac{\sum_{k=1}^{r} \alpha_k x_k}{\sum_{k=1}^{r} \alpha_k} \quad (6)$$

III. USER'S POSITION

The position information could be figured out absolutely or relatively.

The relative position is stated as proximity to the object with a known position in the system. Objects with a known position are called anchor points in the system. This way of how gaining information concerning a position is suitable especially in a Global System for Mobile Communications (GSM) network. Here the user's position is estimated by exploiting the known position of the Base Transceiver Station (BTS), in the network where there is a mobile terminal connected [3]. This kind of localization is mentioned in references [1], [2], [3].

The second way is possible by using an absolute position. Information about the position consists of two or three coordinates. This way is usually used in cartography or in the Global Positioning System (GPS).

In the authentication and authorization process, we can consider both kinds of interpretation concerning the user's position.

In certain cases it is not necessary to use an absolute position. If we know the user is located in the proximity of an anchor point it could be sufficient information. The accuracy of the position information decreases with increasing distance from the anchor point.

In the Figure 4 you can see a basic schematic of the principle of relative positioning, as previously described in [6]. The shaded area is a room covered by the signal from

 ISBN: 978-1-61208-399-5

the anchor point (x_{AP}, y_{AP} and z_{AP} are coordinates of the anchor point's position). Between the authenticator and anchor point there has to be the establishment of mutual trust, it means the authenticator believes in the information form of the anchor point and vice-versa. If the user is in the signal range of the anchor point, it means it has to be able to communicate with the anchor point. If the user's terminal claims to the authenticator it is located near to the anchor point, the authenticator is able to validate this claim by the authenticator.

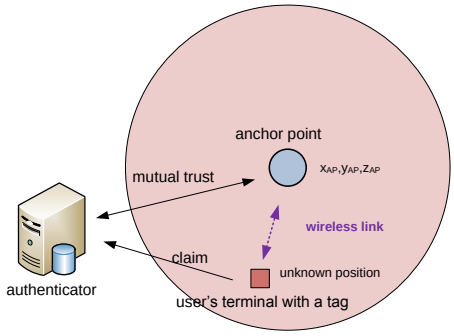

Figure 4. The relative positioning principle

In the rest of the paper we will consider the next sources for localization that could be used as position formation sources in an authentication terminal. For outdoor usage it would be a GPS receiver and a terminal GSM module. Exclusively for indoor usage it will be a module with a wireless interface regards corresponding to IEEE 802.11.

IV. THE AUTHENTICATION SYSTEM

In relation to the previous sections, here is an example of an authentication system concerning the processing of a user's positional information. Below is a list of steps which should be gone through in the design period.

Description - in this step there should be a general description of the behavior of future system.

Authentication techniques - all considered authentication techniques should be considered.

Relations – all relations between used authentication techniques should be specified.

Splitting, used techniques – all listed techniques in the second step should be split into two groups. The first group will be formed by techniques performed in an authentication terminal and the second in an authenticator.

Difficulty – we should imagine how strong each technique is and also how trusted it is as well.

Influences – all the main influences for used techniques, which could have an impact on the authentication process have to be taken into account.

Quantification - all listed influences should receive a value which describes its importance.

Scheme assembly – with regards to the list of authentication techniques, their relations and splitting into two sites schemes of how a whole system could be assembled.

Fuzzyfication – all input and output variables with their influences have to be transformed to linguistic variables

Inference rules – the behavior of the whole system and especially output variables are dependent on used rules.

An example is given below detailing an authentication system which performs a strong authentication where the user's position is one of the processed factors.

A user will use an authentication terminal (Figure 5) to prove its identity to the authenticator. The authentication terminal contains modules for the determination of position such as: GPS receiver, terminal GSM or radio interface IEEE 802.11. Because we need to prove the user's position we have to demonstrate the user is in the same place as the authentication terminal. The authentication terminal uses a fingerprint reader for this task, as well as a tested biometric authentication technique [6]. Positional data is not sent to the authenticator until the fingerprint is checked. The authentication terminal is assigned to the concrete user (it's personalized by a fingerprint and encryption key KEY and password). Data is encrypted by an encryption key (unique for the terminal) is transmitted from the terminal to the authenticator. Note, we assume using AES128 or AES256 as secure enough encryption algorithms [6]. It means each terminal could be used as a unique token in the system and works as an additional authentication factor. Positional data is strongly related to the time when the positional data was created. In the Figure 5 you can see several sources of time information.

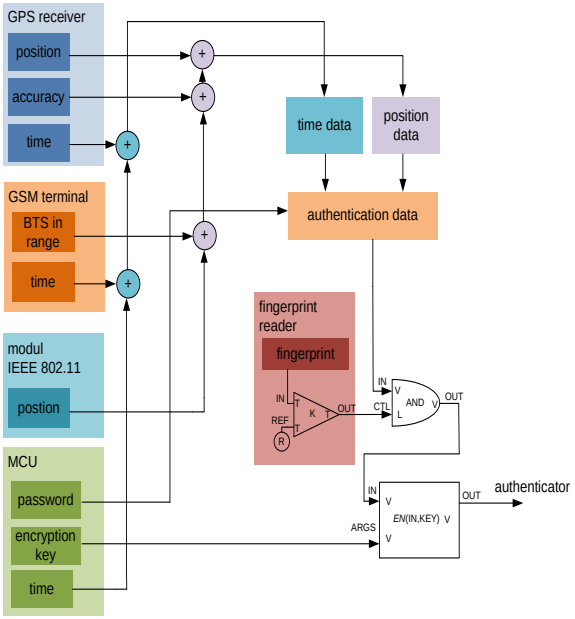

Figure 5. The authentication terminal

The authenticator which stores the user's profile is on the other side. The user's profile holds all the necessary data for the user for defined locations (from where the user could be authenticated), encryption key, password etc. The schematic of the authenticator is illustrated in Figure 6. All necessary data is stored in a knowledge base, also *inference rules* or amplification coefficients A_X. Each subsystem on Figure 6 is a fuzzy system which performs the authentication of a specific factor (for example, *subsystem GPS* processes data from the GPS receiver).

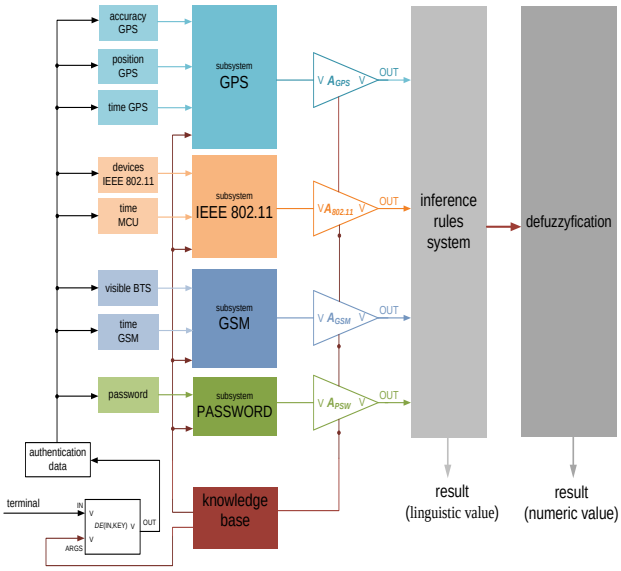

Figure 6. The authenticator

The behavior of the whole system is defined by inference rules which are part of the knowledge base. The rule is described in section 2 and it usually takes the form of a "if then" condition. Table 1 lists the top level rules for the authenticator for evaluating the state of positional information.

TABLE I. THE INFERENCE RULES

Trust GPS	Trust GSM	Trust IEEE 802.11	Position
high			well proved
low	high	high	well proved
low	low	low	not proved
low	moderate	low	not proved
low	high	low	proved
low	low	high	proved

The result of the processing of the submitted authentication data is the level of trust that the user has identified which he claims and he is in the location where he claims. How the level is varied with different input data can be seen in Figure 7. The result in Figure 7 is based on the application inference rules set (table 1) and provided by Matlab. There we can see how trust concerning positional information $\delta_{POSITION}$ is dependent on the results from the subsystems, in this case from the GSM subsystem δ_{GSM} and the IEEE 802.11 subsystem $\delta_{IEEE80.11}$. We can see the highest value of $\delta_{POSITION}$ is in the case when both of the input values are also in high values. This is the simplest example of dependence but could vary with different inference rules according to authentication system requirements.

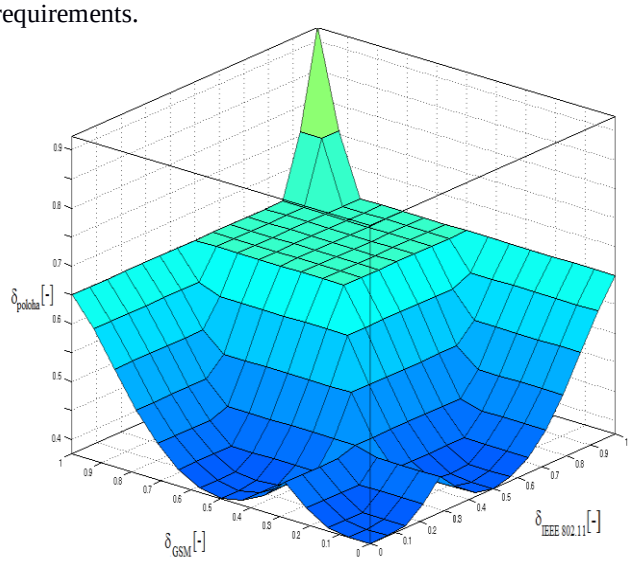

Figure 7. The trust to position information

The development board was designed for an authentication terminal (Figure 8). The board is based on 16-bit RISC (Reduced Instruction Set Computing) microcontroller MSP430F5529 from Texas Instruments and is equipped with a new version of eMMC memory, where all required data are stored. The board contains IEEE 802.11 radio interface RN131C from ROVING.

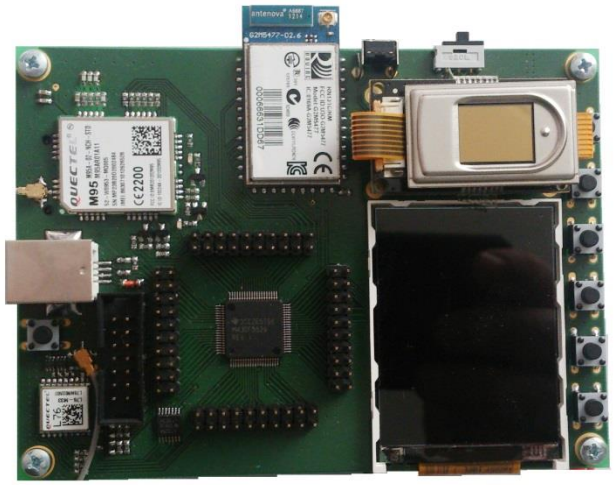

Figure 8. The Authentication terminal development board

 ISBN: 978-1-61208-399-5

This radio is able to list Media Access Control (MAC) and addresses devices in the neighborhood with their appropriate Received Signal Strength Indication (RSSI). Two modules have been chosen from Quectel. The first one is the GPS receiver L76 and the second one is the GSM module M95. The board is equipped with five buttons, user defined functions and an LCD with a resolution of 240 x 320 pixels. As was mentioned previously the board contains a fingerprint reader: FPC-AM3 from Fingerprint.

V. CONCLUSION

The article deals with the possibility of using fuzzy logic principles in the authentication process in a computer network environment. The basic idea is make the result of the authentication process more diffusive with regards to vague input data (authentication factors). Presently systems produce a result in bivalent logic as “Yes/No” or “True/False”. In many cases the right one is somewhere in the middle. This could be correct especially in the evaluation of positional information, this means where an authenticated user is located. This information could be unclear or inaccurate and therefore, the result will also be unclear or inaccurate. Fuzzy logic could represent a possible way of how to control a system with vague values.

The focus is on positional information. We introduce a GPS receiver or GSM terminal as positional information sources in the authentication process. We also introduce the idea of relating positional information with a human biometric element for strong authentication (the user has to be in the same place as the authentication terminal).

Next, the paper presents a possible way of how to set up a basic authentication model step by step. Further to this the example of an authentication system is presented. For testing purposes the development board of an authentication terminal was designed and realized.

Future work will be aimed at testing the presented principles in a real environment. Although the basic principles were verified in a previous version of an authentication terminal, our next work will focus on the implementation of advance techniques related to positional information.

ACKNOWLEDGMENT

Research described in this paper was financed by the TA04010476 project TACR "Secure Systems for Electronic Services User Verification" and by the Czech Ministry of Education in the framework of the National Sustainability Program under the grant LO1401. For research, infrastructure of the SIX Center was used.

REFERENCES

[1] W. de Ru, J. H. P. Eloff, "Enhanced Password Authentication through Fuzzy Logic," , 1997.

[2] Kwang H. Lee, First Course On Fuzzy Theory and Application. Berlin: Springer-Verlag, 2005.

[3] M. Ibrahim and M. Youssef, "A Hidden Markov Model for Localization Using Low-End GSM Cell Phones," in Communications (ICC), 2011 IEEE International Conference, 2011, pp. 1-5.

[4] N. Deblauwe and G. Treu, "Hybrid GPS and GSM localization — energy-efficient detection of spatial triggers," in Positioning, Navigation and Communication, 2008, pp. 181-189.

[5] A. Goetz, S. Zorn, R. Rose, G. Fischer, and R. Weigel, "A time difference of arrival system architecture for GSM mobile phone localization in search and rescue scenarios," in Positioning Navigation and Communication (WPNC), 2011, pp. 24-27.

[6] D. Jaros, R. Kuchta, R Vrba, "The Location-based Authentication with The Active Infrastructure," in : The Sixth International Conference on Internet and Web Applications and Services, Sint Maarten, 2011, pp. 228-230.

[7] A. K. Jain. On The Uniqueness of Fingerprints. [retrived: January, 2015],[Online].http://biometrics.cse.msu.edu/Presentations/AnilJain_UniquenessOfFingerprints_NAS05.pdf

[8] A. Bogradlow, D. Khovratovich, Ch. Rechberger. Biclique Cryptanalysis of the Full AES[retrived: January, 2015], Research Microsoft. [Online]. http://research.microsoft.com/en-us/projects/cryptanalysis/aesbc.pdf

 ISBN: 978-1-61208-399-5