Towards the Attack Signatures' Comparison in Survivable Computer Networks

Milos Manic
Department of Computer Science
University of Idaho
800 Park Blvd. Ste.#200
Boise, ID 83712, USA
misko@ieee.org

Bogdan Wilamowski
College of Engineering
University of Idaho
800 Park Blvd. Ste.#200
Boise, ID 83712, USA
wilam@ieee.org

***Abstract* – Survivability architecture and run-time attack detection can be successfully implemented based on attack signatures. In this paper, authors concentrate on profile signatures based on Markov models. They are represented by the frequency spectrum of the functionalities in the system. The difference between safe system signatures from attacked (monitored) system signatures indicates possible intrusion. This paper proposes an approach, based on soft computing techniques, for recognizing that difference.**

I. INTRODUCTION

The malicious act research is usually represented by 3R's: recognition, resistance and recovery. Resistance describes hardening the system against hacker attacks. Recognition aims in intrusion detection. Recovery deals with ways of surviving malicious acts. The survivability is considered to be a combination of recognition and recovery steps. In case of survivability, recognition can be omitted in case of solely fault masking objective. This paper deals with computer/network survivability and fault-tolerant systems that, in spite of their probabilistic malicious attack features, have the same goal.

Attack signatures could be captured in many ways. Commercial intrusion detection software comes with a number of signatures, with the ability for customers to modify or add their own signatures. They come verified, tested and digitally signed for authentication [1]. In this paper authors concentrate on profile-based signatures based which are based on Markov models. Signatures are represented by frequency spectrum of the functionalities in system. Functionalities are particular user actions, like logging procedures, or other usage of services, relevant for the purpose of behavior profiling. Difference of the signature of attacked monitored system and "safe" one indicates possible intrusion.

This paper proposes a possible approach to a process of differentiation between signatures of normal and attacked behavior of a monitored system and is inspired by the concept proposed in [2]. The paper describes difficulties in differentiating normal signatures and signatures in a system under attack.

Quantitative numerical methods applied traditionally are not offering satisfying results. Soft computing techniques, namely fuzzy logic, lead to more qualitative depiction of data by its inherent linguistic manner of data compression. Fixed thresholds may lead to false alarms or to low sensitivity to actual ones. Adaptive thresholds, on the other hand, may result in slow changes in the system and therefore unnoticed intrusion.

An adaptation problem (false positives) could be solved with limiting the scope of adaptation upfront. This process can be carried out either by using expert knowledge or by monitored behavior of the system. This behavior depends on the time when system is used, number of users, etc. Thereby slow drift towards undetected attacks on one hand is disabled. On the other hand the necessary level of adaptation implemented in form of fuzzy rules is enabled.

The main advantage of the proposed approach is the ability of comparison of two attack signatures regardless of their shape. The method takes into consideration both the shape and mutual position of two signatures. It also proposes ideas for adaptability that would enable sensitivity and avoid false alarms at the same time, therefore elude the danger of slow shift to malicious behavior. This method gives the comparison of points of gravities, i.e. takes equally into a consideration all frequencies from the attack signature.

As a consequence, the feature that could be understood as both an advantage and a disadvantage emerges from this method. System signature frequencies on a right side have more "weight" than ones on the left side. If the importance of frequencies, i.e. certain system functionalities, is not sorted out in ascending order, meaning growing while going from left to right side of signature, method proposed in this paper has to be upgraded to take those weight arrangement into account. Otherwise, for two totally different but mirror like symmetrical signatures, this method could return equality.

A second disadvantage of this method is less influential and originates from a nature of fuzzy operators. Fuzzification of attack signatures must be carried out in such a way that this fuzzy signature has zero values only in boundary, left and right, points. Otherwise, an attack signature would be interpreted as a sequence of fuzzy values. This modification is relatively insignificant for each signature especially since it is applied to both compared signatures.

II. MOTIVATION

The motivation for attacking problems of survivability and fault tolerance through attack signatures has several reasons. Identification of critical functionalities of the system is more cost efficient then the approach that encompasses complete system. Therefore, more optimized solution can be achieved by focusing on critical functionalities as identified by means of attack signatures [2].

On the other hand, methods for ranking fuzzy numbers are experiencing growing interest. An approach taken in this paper relies on an isolation of functionalities affected by

malicious attacks. Those functionalities are recorded by means of attack signatures that are converted to fuzzy sets.

This paper applies fuzzy preference relation comparison techniques [3, 4, 5] on signature attacks. Existing relations considered fuzzy numbers, that are convex and normalized sets. This approach uses signatures that can include zero values. That is why method works on arbitrary sets – fuzzy values.

Latest approaches in literature assumed idle state as the state not affected by users behavior or by some applications. This can lead to false alarms/lack of sensitivity [6, 7, 8]. Careful introduction of adaptability, based on qualitative rules might be an approach for resolving this problem [9, 10]. In literature different approaches to a problem of an adaptive fault tolerance can be found [11]. This paper is not considering a problem of adaptability limitation. Rather, authors present ideas that are applicable with the proposed method of comparison two signature attacks.

The rest of this paper is structured as follows. The third and fourth section proposes soft computing approach. The fifth section provides the test example results. The sixth section explains possible methods of signature attacks fuzzification. The seventh section concludes this paper with directives for future work.

III. FUZZY EXTENSION OF CLASSICAL PREFERENCE STRUCTURES

Fuzzy preference structure on a set of signatures *A* is a triplet $\Pi_{\varnothing} = (P, I, R)$ which can be characterized by the unique binary relation *S* in A. This relation is called characteristic preference relation. Preference relation *S(a,b)* represents the degree to which an alternative a is at least as good as alternative *b*.

The satisfaction degree $S_\gamma(A_i > A_j)$ of the comparison of two fuzzy numbers $A_i > A_j$ can be regarded as the preference degree of A_l to A_j. Let the set $\mathscr{A} = \{A_1, A_2, ..., A_n\}$ be a set of fuzzy numbers that might be the evaluations for the signatures to be compared. Then a fuzzy preference relation R_s, with respect to the satisfaction function S_γ, can be defined as follows:

$$R_s : \mathscr{A} \times \mathscr{A} \to [0,1]. \tag{1}$$

The fuzzy preference relation $R_s(A_i, A_j)$ indicates the degree to which fuzzy number A_i dominates fuzzy number A_j.

Different approaches to fuzzy preference relation construction exist in literature [12]. One of the earliest concepts is Orlovsky's fuzzy preference relation :

$$R_s(A_i, A_j) = \begin{cases} S_\gamma(A_i > A_j) - & \text{when } S_\gamma(A_i > A_j) \geq \\ -S_\gamma(A_j > A_i), & \geq S_\gamma(A_j > A_i) \\ 0, & \text{otherwise} \end{cases}. \tag{2}$$

Lee with associates [4] has proposed the following fuzzy preference relation:

$$R_s(A_i, A_j) = S_\gamma(A_i > A_j) + \tfrac{1}{2} S_\gamma(A_i = A_j). \tag{3}$$

They have also proved next two frequently used properties of fuzzy preference relations:

$$R_s(A_i, A_j) + R_s(A_j, A_i) = 1, \quad \forall A_i, A_j \in \mathscr{A}. \tag{4}$$

$$R_s(A_i, A_i) = 0.5, \quad \forall A_i \in \mathscr{A} \tag{5}$$

IV. FUZZY SATISFACTION FUNCTION

Fuzzy number *A* is a fuzzy set defined in the real domain *R*. Its membership function fulfills conditions of convexity, normality and continuity on the universe of discourse. In this paper the shape of attack signatures is considered to have a continual form.

The satisfaction degree of an arithmetic comparison of two fuzzy numbers is exploited in constructing fuzzy preference relation. This degree is calculated by using a fuzzy satisfaction function [4].

Fuzzy satisfaction function $S_\gamma(A_i < A_j)$ is defined as:

$$S_\gamma(A_i < A_j) = \frac{\sum_{x=I_{\min}}^{I_{\max}} \sum_{y=J_{\min}}^{\min\{x-\gamma, J_{\max}\}} \mu_{A_i}(x) \Theta \mu_{A_j}(y)}{\sum_{x=I_{\min}}^{I_{\max}} \sum_{y=J_{\min}}^{J_{\max}} \mu_{A_i}(x) \Theta \mu_{A_j}(y)}, \tag{6}$$

where $I_{\min} = \min D_\gamma(A_i)$, $I_{\max} = \min D_\gamma(A_i)$, holding the condition that '$a \Theta b > 0$ *if* $a > 0$ *i* $b > 0$ (Θ denotes one of possible different operators on fuzzy sets).

The equality comparison $S_\gamma(A_i = A_j)$ has the following form:

$$S_\gamma(A_i = A_j) = \frac{\sum_{x=\max\{I_{\max}, J_{\max}\}}^{\min\{I_{\max}, J_{\max}\}} \mu_{Ai}(x) \Theta \mu_{A_j}(y)}{\sum_{x=I_{\min}}^{I_{\max}} \sum_{y=J_{\min}}^{J_{\max}} \mu_{A_i}(x) \Theta \mu_{A_j}(y)}. \tag{7}$$

The satisfaction function S_γ has the following properties:

1. $S_\gamma(A_i = A_j) + S_\gamma(A_i < A_j) + S_\gamma(A_i > A_j) = 1$
2. If $\max\{D_\gamma(A_i)\} < \min\{D_\gamma(A_j)\}$, then $S_\gamma(A_i < A_j) = 1$.
3. If $A_i \equiv A_j$, then $S_\gamma(A_i < A_j) = S_\gamma(A_i > A_j)$
4. For any two fuzzy numbers A_i and A_j $0 \leq S_\gamma(A_i < A_j) \leq 1$

($A_i \equiv A_j$ means that the shapes of two fuzzy values are the same (i.e. $\mu_{A_i} = \mu_{A_j}$), while in formula $S_\gamma(A_i = A_j)$ symbol = means that two fuzzy values represent the same **actual** value - $av(A_i) = av(A_j)$).

From the above, it is clear that the less two fuzzy values are overlapped, the satisfaction degree is closer to 1 or 0.

V. EXPERIMENTAL RESULTS

Test examples have included cases of various mutual positions of two fuzzified attack signatures. Signatures represented by fuzzy sets A_1 and A_2 are investigated with the overlapping factor from 0% over maximal overlapping percentage to 0% again (Fig. 1). This means that fuzzy satisfaction function and therefore fuzzy preference relation is calculated over the fuzzy values that change their position in following way: second signature is in fixed position, while the first one shifts from being connected on the right hand side to a second one, to being connected in another spot, but on the other side. A case of separated fuzzy values is not considered because of its simplicity. In that case values of fuzzy preference relation are obviously either 1 or -1.

Example shows smoother changes of fuzzy preference relation values for overlapping for intersection operators than for union operators. Union operators result in discontinued changes in fuzzy preference relation values.

Fig. 1 shows values of a fuzzy preference relation moving from 0 to 1, for overlapping from 0% over max% to 0%. These values are obtained for test example depicted by Fig. 2.

Overlapping factor of fuzzified attack signatures A_i and A_j is calculated by formula:

$$\frac{A_i \cap A_j}{A_i \cup A_j} \cdot 100\%, \tag{8}$$

where $\cap$ and $\cup$ are defined as in [13]:

$$F \cup G = \int_U (\mu_F(u) \vee \mu_G(u)) / u \cdot \tag{9}$$

VI. CONVERSION OF ATTACK SIGNATURES TO FUZZY VALUES

The conversion deals with the determination of membership functions. This can be easily done in number of ways. Methods that could be applied are three-phase, incremental, multiphase fuzzy statistical method, and others [14].

For the specific case of an abrupt increase/decrease of function traced by values of frequencies, interpolating polynomials would suffer oscillations. In contrast, due to its limitation to third-order curves with smooth transitions, cubic spline provides much more acceptable approximation [15].

Since the partial attack signature is known, simple interpolation (curve fitting) could be used to obtain certain fuzzy value (set) out of partial signature Si. This topic is outside of this paper and will not be further discussed. However, the precision of this conversion might have crucial influence on final results.

Attack signature corresponding to an A_i which is an atomic, smallest attack, unit is given on Fig. 1. An example of approximating fuzzy value upon given determined partial attack signature is also given on same figure.

The results of Lee's fuzzy preference relation given by equation (3) are presented for the above example in Fig. 2.

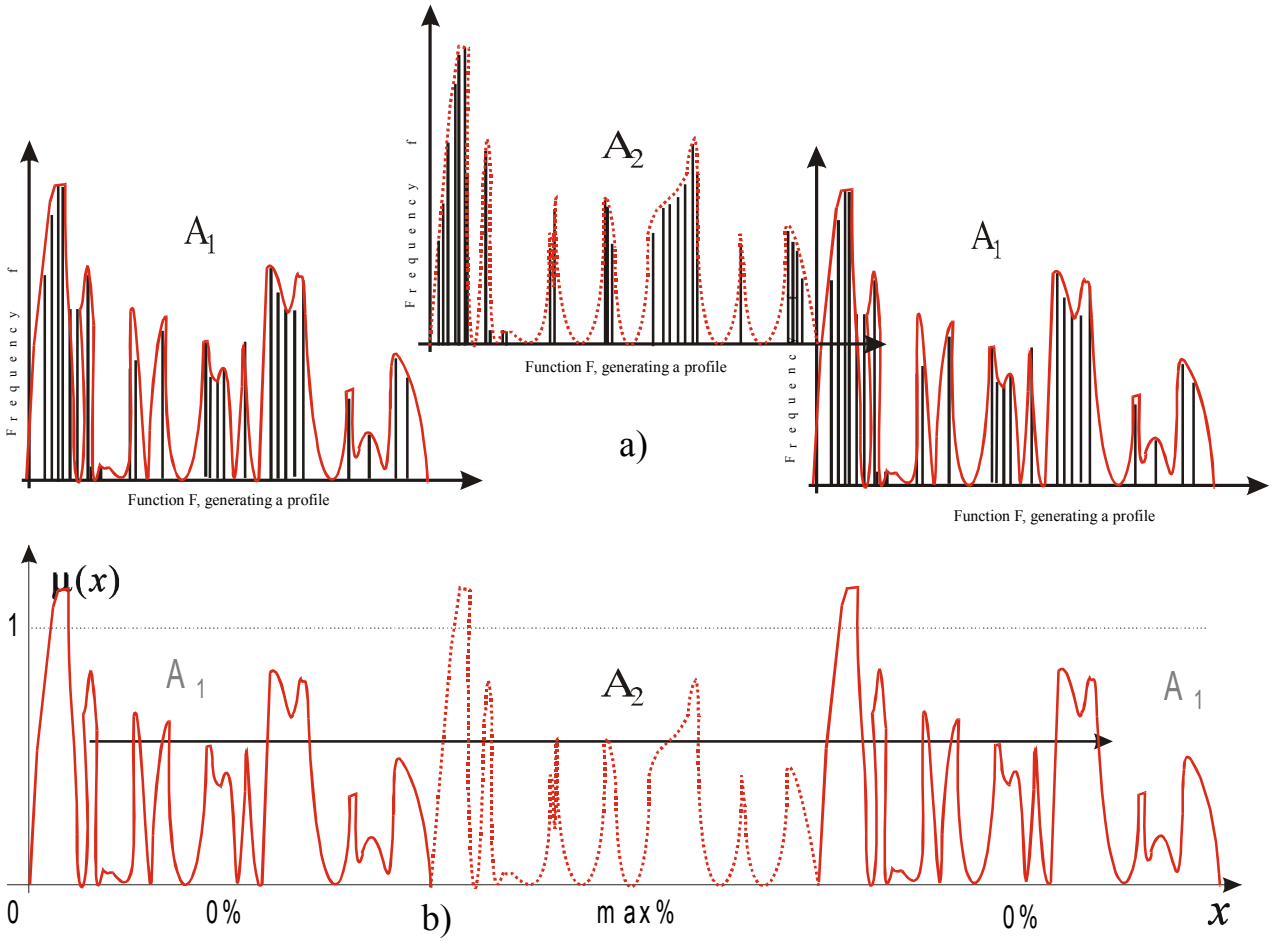

Fig. 1. a) Two attack signatures, and their correspondent fuzzy value
b) Example of comparison of two attack signatures

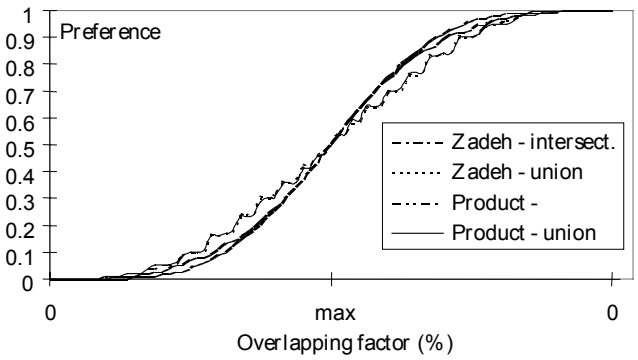

Fig. 2. Lee's fuzzy preference relation depending on an overlapping extent and a shape of attack signatures, for the test example above

VII. CONCLUSION

The main advantage proposed in this paper is the ability of comparison of two attack signatures regardless of their shape. This method takes into consideration both the shape and mutual position of two signatures. Two non-overlapping signatures is considered as trivial case (one is obviously "stronger" than the other). Attack signatures are derived to isolate operating system or application functions. Fuzzy preference relation with different operators is proposed for capturing the difference between signatures.

Two disadvantages of this method are noticed. First one is that weight of frequencies has to be sorted out in ascending order. Otherwise, for two totally different but mirror like symmetrical signatures, in certain cases method could return equality. Second disadvantage of this method is that fuzzified attack signatures can have zero values only in boundary, left and right, points. Otherwise, one signature will be interpreted as a sequence of fuzzy values. This change is relatively insignificant for each signature especially since applied to both values.

VIII. FURTHER WORK

Threshold adaptability by means of fuzzy rules could avoid both false alarms and lack of sensitivity [6, 7, 8]. Adaptability could be allowed in terms of qualitative description of signatures. Those descriptions should reflect period of day of network usage, number of users, etc. This automated restriction of a possible adaptability extent is one of the further goals of authors.

Method could be upgraded to take "weights" of frequencies into account.

Off-line derivation process generating attack signatures can be implemented on-line with adaptive idle system signature. This issue is to be cautiously addressed.

IX. REFERENCES

[1] Internet Security Systems URL: http://www.iss.net/.

[2] A. Krings, S. Harrison, J. Dickinson, M. McQueen, "Survivability of computers and Networks based on Attack Signatures", *Proc. 3rd Information Survivability Workshop, (ISW-2000)*, Boston, Massachusetts, October 24-26 2000, pp. 91-94.

[3] J.J. Buckley, "Ranking alternatives using fuzzy numbers*"*. *Fuzzy Sets and Systems 15*, 1985, pp. 21-31.

[4] K.M. Lee, C.H. Cho, H.L. Kwang. "Ranking fuzzy values with satisfaction function", *Fuzzy Sets and Systems* 64, 1994, pp. 295-309.

[5] M. Manic, S. Milutinovic, "Fuzzy preference relation depending on different operators and fuzzy numbers", ***I**nternational **F**uzzy **S**ystems **A**ssociation, IFSA '97,* Prague, June 25-29, 1997, pp. 64-69.

[6] M. Manic, "Alarm systems for monitoring driven by fuzzy logic", ***P**reventive **E**ngineering & **I**nformation **T**echnologies*, Nis, 8.-10. December 1994, pp. 30.1-30.4.

[7] E. Cox, "Adaptive Fuzzy Systems", *IEEE Spectrum*, Febr.1993, pp. 27-31.

[8] C.T. Sun, "Rule-Base Structure Identification in an Adaptive-Network-Based Fuzzy Inference System", *IEEE Trans. on Fuzzy Syst.*, vol.2, no.1, Feb. 1994, pp. 64-73.

[9] M. Manic, "Fuzzy-Operators Weight Refinements", *IEEE Annual Reliability & Maintainability Symposium, RAMS'99*, Washington, DC USA, January 18-21 1999, pp. 245-251.

[10] S. Milutinovic, M. Manic, M.S. Stankovic, "Influence of choosing operators on preference of fuzzy numbers", *The Second Workshop on **FU**zzy **B**ased **E**xpert **S**ys**T**ems, FUBEST '96*, Sofia, Oct. 9-11 1996.

[11] K. Kim, T. Lawrence, "Adaptive fault tolerance in complex real time distributed applications", *Computer Communication*, vol 15, no 4, 1992, pp. 243-251.

[12] S. Zahariev, "On Orlovsky's definition of nondomination". *Fuzzy Sets and Systems* 42, 1991, pp. 229-235.

[13] A.L. Zadeh, "Appendix", *Proc. of the U.S.-Japan Seminar on Fuzzy Sets and Their Application*, Berkeley, Ca., July 1974, pp. 27-39.

[14] H.X. Li, V.C. Yen, *Fuzzy sets and fuzzy decision making*, CRC Press, 1995.

[15] S.C. Chapra, R.P. Canale, *Numerical Methods for Engineers*, 3rd ed., McGraw Hill Companies 1998.