Contextual Fuzzy Cognitive Map for Intrusion Response System

Montaceur Zaghdoud*
Department of Information System
College of Computer Engineering and Sciences,
Salman bin Abdulaziz University, Al Kharaj, KSA
*zaghdoud {at} sau.edu.sa

Mohammed Saeed Al-Kahtani
Department of Computer Engineering
College of Computer Engineering and Sciences,
Salman bin Abdulaziz University, Al Kharaj, KSA

Abstract- **An intrusion response system is charged with minimizing any losses caused by intrusion. It remains ineffective if the response to the intrusion does not bring the timely and adequate corrections required by the victim system. This paper proposes a new intrusion response system based on contextual fuzzy cognitive map. In this intrusion response system framework, a new ontology is defined based upon conceptual graphs in order to describe relationships between different intrusion concepts and recognize suspect connection as an intrusion which belongs to known intrusion class (DOS, PROBING, U2R or R2U). Fuzzy cognitive maps are used to assess the negative impact of an intrusion on the victim system. Specifying appropriate remedies for all damages which are caused by intrusion is considered as main task of intrusion response system. There are two kinds of remedies: direct or indirect remedies, the former is accomplished by acting directly on the victim system but the later is considered as remotely acting on damaged system. The proposed intrusion response system is multilayer system. The first layer is charged with the identification of the intrusion suspect intrusion using conceptual graphs to build a new ontology. The second layer assesses the effect of intrusion on the victim system using a fuzzy cognitive map. The third layer recommends a response in two ways: automatically by acting through a mobile agent, or manually by alerting the appropriate security administrator.**

Keywords-contextual fuzzy cognitive map; conceptual graph, fuzzy cognitive map, intrusion detection; intrusion response; mobile agent.

I. INTRODUCTION

Intrusion detection is the process of monitoring the events occurring in a computer system or network and analyzing them for signs of possible incidents, which are violations or imminent threats of violation of computer security policies, acceptable use policies, or standard security practices [25]. Intrusion detection action remains ineffective if it's not followed by a convenient response to the intrusion and if it is not able to bring solutions of the damages affecting the target system of an attack. Intrusion detection can be defined as the process of identifying malicious behavior that targets a network and its resources [20]. Malicious behavior is defined as a system or individual action which tries to use or access to computer system without authorization and the privilege excess of those who have legitimate access to the system. The term *attack* can be defined as a combination of actions performed by a malicious adversary to violate the security policy of a target computer system or a network domain [7]. Each attack type is characterized by the use of system vulnerabilities based on some feature values. Usually, there are relationships between attack types and computer system characteristics used by the intruder [14].

Besides, anti-intrusions system should take into account uncertainty that can affect intrusion data. Uncertainty on parameters can have two origins [4]. The first source of uncertainty comes from the uncertain character of information that is due to a natural variability resulting from stochastic phenomena. This uncertainty is called variability or stochastic uncertainty. The second source of uncertainty is related to the imprecise and incomplete character of information due to a lack of knowledge. This uncertainty is called epistemic uncertainty. The systematic utilization of a unique probability distribution to represent this type of knowledge supposes a too rich subjective information and risk to be in part arbitrary [14].

Intrusion response system proposed in this paper uses a response strategy based on three steps: intrusion recognition, intrusion degas definition and intrusion response. Intrusion detection is the responsibility of IDS. After detecting intrusion the proposed response strategy may recognize intrusion nature among four known classes: DOS, PROBING, R2L and U2R. In this second step we use ontology based on conceptual graphs. The third step is charged by defining possible damages caused by intrusion on target

computer/information system using fuzzy cognitive map. The final step of proposed response strategy should make valuable direct or indirect response by sending advising message to system administrator or by charging mobile agents by appropriate remedies and correctives.

II. INTRUSION DATA AND CLASSES

In this paper and also in our last papers [2,14,15,16] which are related to this work, we used DARPA KDD'99 dataset which is counting almost 494019 of training connections [8,9]. Based upon a discriminate analysis, we used data about only important features (the 9th first features):

- Protocol type: type of the protocol, e.g. tcp, udp, etc.
- Service: network service on the destination, e.g., http, telnet, etc.
- Land: 1 if connection is from/to the same host/port; 0 otherwise.
- Wrong fragment: number of ``wrong'' fragments.
- Num_failed_logins: number of failed login attempts.
- Logged_in: 1 if successfully logged in; 0 otherwise.
- Root_shell: 1 if root shell is obtained; 0 otherwise.
- Is_guest_login: 1 if the login is a ``guest'' login; 0 otherwise.

DARPA'99 base counts 38 attacks which can be gathered in four main classes:

- Denial of Service (DOS): Attacker tries to prevent legitimate users from using a service.
- Remote to Local (R2l): Attacker does not have an account on the victim machine, hence tries to gain access.
- User to Root (U2R): Attacker has local access to the victim machine and tries to gain super user privileges.
- Probe: Attacker tries to gain information about the target host.

III. INTRUSION DETECTION AND PREVENTION SYSTEM

Intrusion detection concept is due to James Anderson's paper published in 1980 and titled “Computer Security Threat Monitoring and Surveillance”. In 1988, at least three IDS prototypes were created [5, 6, 28]. Since then, several significant events in intrusion detection technology have contributed to the evolution of Intrusion Detection System (IDS).

IDSs are usually classified as host-based or network-based. Host-based systems use information obtained from a single host (usually audit trails), while network based systems obtain data by monitoring the trace of information in the network to which the hosts are connected [22].

Intrusion detection is classified into two types: misuse and anomaly detection. Misuse intrusion detection uses well-defined patterns of the attack that exploit weaknesses in system and application software to identify the intrusion. These patterns are encoded in advance and used to match against the user behavior to detect intrusion. Anomaly intrusion detection uses the normal usage behavior patterns to identify the intrusion [23].

Network intrusion detection devices intercept packets traveling along various communication mediums and protocols, usually TCP/IP. Captured packets are analyzed in a number of different ways. Some NID devices will simply compare the packet to a signature database consisting of known attacks and malicious packet "fingerprints", while others will look for anomalous packet activity that might indicate malicious behavior.

When referring to network-based security techniques, the term *network intrusion prevention* is usually applied to an *inline* device (such as an Ethernet bridge or firewall) that has the capability of modifying or discarding individual attack packets as they traverse the device interfaces. Unfortunately, this term has been redefined and abused by marketing and sales teams to the point that many security professionals have an allergic reaction when hearing it and refuse to have anything to do with it [24].

Intrusion detection and prevention systems (IDPS) are primarily focused on identifying possible incidents, logging information about them, attempting to stop them, and reporting them to security administrators [25]. IDPSs are primarily focused on identifying possible incidents. For example, an IDPS could detect when an attacker has successfully compromised a system by exploiting vulnerability in the system. The IDPS could then report the incident to security administrators, who could quickly initiate incident response actions to minimize the damage caused by the incident [25].

Intrusion Detection Systems can be classified according to activity:

- **Passive:** Passive IDS detects and records intrusion attempts, but it does not take action to minimize damage already caused by the attack or prevent

further attacks. Their main goal is to notify the authority and/or provide attack information.

- **Active:** As opposed to passive systems, an active IDS aims to minimize the damage done by the attacker and/or attempt to locate or harm the attacker. Active IDS detects the attacks and sends an alert to the network administrator or take action to block the attack.

The majority of the existing intrusion detection systems provide passive response [33].

This paper deals with intrusion prevention and/or counter-attack measures based upon a response strategy as complement of a research work undertaken by our research team and described in our last papers [14,15,16].

IV. INTRUSION RESPONSE SYSTEMS

Intrusion Response systems can be classified according to level of automation:

- *Notification systems:* Notification systems mainly provide information about the intrusion which is then used by the system administrator to select an intrusion response. The majority of existing IDSs provide notification response mechanisms.
- *Manual response systems:* Manual response systems provide higher degree automation than notification-only systems and allow the system administrator to launch an action from a predetermined set of responses based on the reported attack information.
- *Automatic response systems*: As opposed to manual and notification approaches, automatic response systems provide immediate response to the intrusion through an automated decision making process.

Although today intrusion detection systems are greatly automated, automatic intrusion response support is still very limited [33].

This work belongs to active IDS and notifying/automated IRS. Response could be by notifying administrator or automated by charging mobile agent with damage repairs of victim computer network or information system. Active intrusion response reaction in this paper is guided by response strategy based on three steps: intrusion recognition, intrusion degas definition and intrusion response.

Once the intrusion was detected, the system proceeds by recognizing intrusion nature among four known classes: DOS, PROBING, R2L and U2R. We use ontology which describes how intrusion can belong to a class or another based on conceptual graphs.

The second step is charged by defining possible damages caused by intrusion on victim computer/information system using fuzzy cognitive map which describes possible influences between components of victim system. The third and final step of proposed response strategy should make valuable direct (automated) or indirect (not automated) response by sending advising message to system administrator or by charging mobile agents by appropriate remedies and correctives.

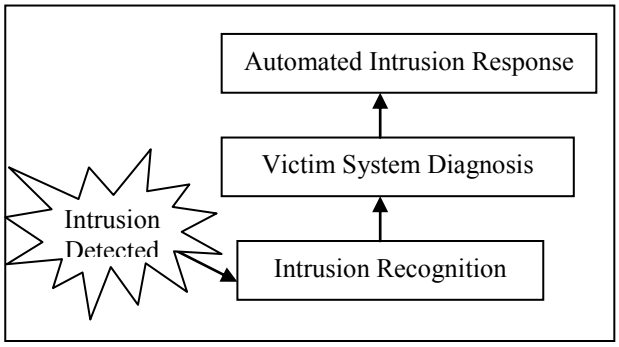

Figure 1: Intrusion Response Strategy

V. INTRUSION RESPONSE SYSTEM ARCHITECTURE

Ambareen Siraj developed an intrusion detection system based on fuzzy cognitive map for misuse detection which involves the comparison of a user's activities with the known behaviors of attackers attempting to penetrate a system. This system uses rule-based detection mechanisms that work on each of the hosts of network. Output from the misuse detection modules may be module is binary.

For other types of attacks like the number of failed logins, the output of the misuse detection module is a fuzzy measure of the degree of suspicion. The decision engine must assess results of the multiple misuse detection modules in order to compute the alert status for each machine and for each user account [27].

In this paper we propose an intrusion response system which is structured within three layers to make an appropriate response for a detected and/or upcoming intrusion. This system uses information which are coming from a forerunner intrusion detection system. The first layer of this multilayer response system is concerned by recognition of intrusion by classifying it in one of four known classes: DOS, PROBING, R2L and U2R. Intrusion recognition task is accomplished using an ontology based on conceptual graph. Intrusion

classification step allows system to know the class to which belongs intrusion.

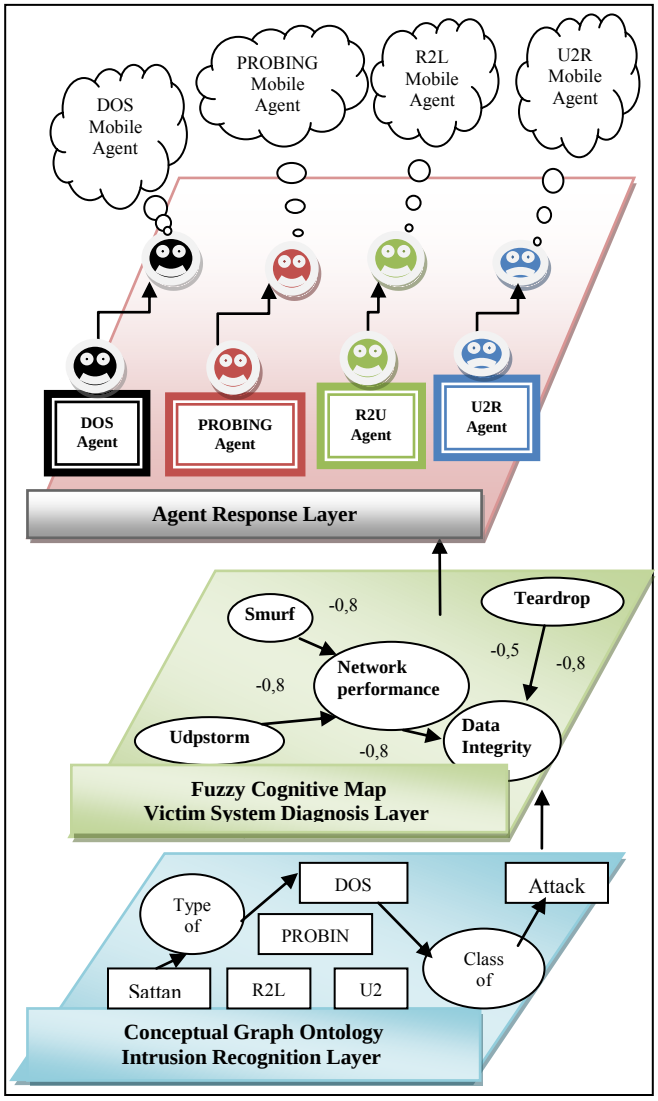

Figure 2: Architecture of Contextual Fuzzy Cognitive Intrusion Response System.

The second layer is charged by knowing influences of intrusion impacts on target system components. Fuzzy cognitive map are used in this purpose. This layer is named diagnosis layer which analyzes effect of intrusion on target system.

The final layer is the third layer which interfaces intrusion response system with victim system administrator. It deals with potential reactions required to counter target system intrusion possible damages. Information about intrusion class comes from first layer to specialized Agents (DOS, PROBING, R2L and U2R) which are charged by sending alert message to target system administrator and/or execute preventive and /or corrective commands on distant intrusion target system.

Mobile agents of this third layer can perform another kind of reaction when it's necessary. They move to intrusion target system and logged into it in order to execute convenient preventive and/or corrective commands which make off intrusion effects.

A. Conceptual Graph Intrusion Recognition Layer

As mentioned before, the first layer of the Cognitive Intrusion Response System is concerned by definition of intrusion class. This layer is the boundary component of the cognitive intrusion response system which allows it to be coupled with an IDS system. When IDS detects or forecasts an incoming intrusion, knowing the class to which intrusion belongs can help us to define convenient response based on effect analysis or diagnostic of intrusion target system. In this research work, intrusion class definition is computed using conceptual graph ontology.

1) Conceptual Graph

The conceptual graph can represent any knowledge if it can be described using concepts and relationships between them. It is also known to be equivalent to the first order predicate logic. Though it loses some information at the moment, it seems to be best suited to our propose knowledge representation [6].

The main foundation is to define a concept and a relation. A concept can be an object, thing, or action. A relation is semantic of how one concept is related to another concept [29, 30, 31]. The notations that Sowa used in his conceptual structures are box, circle, and arrow. A box is used for a concept, a circle for a relation, and an arrow shows the direction of such relation [6]. An example of conceptual graph is shown as follow:

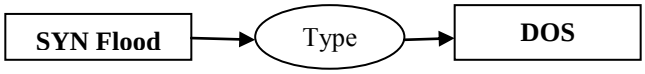

Figure 3: Example of Conceptual Graph relation.

This example indicates that SYN Flood attack is a DOS intrusion

2) Contextual Intrusion Recognition using Conceptual Graph Ontology

In the 1980's the AI community came to use the term ontology to refer to both a theory of a modeled world (e.g., a Naïve Physics [13]) and a component of knowledge systems. Some researchers, drawing inspiration from philosophical ontologies, viewed computational ontology as a kind of applied philosophy [29]. In the context of computer and information sciences, ontology defines a set of representational primitives with which to model a domain of

knowledge or discourse. The representational primitives are typically classes (or sets), attributes (or properties), and relationships (or relations among class members). In typical ontology formalisms one would be able to say that an individual was a member of class [12].

In this paper, we use conceptual graph to represent intrusion relationships which can show possible relation between intrusion and type or class of intrusion (DOS, PROBING, U2R, R2U). Figure 4 shows an illustration of this application. It describes relationship between concepts: Iswep, Mscan, Nmap, Saint and satan are types of intrusion class probing. Probing is a class of Intrusions.

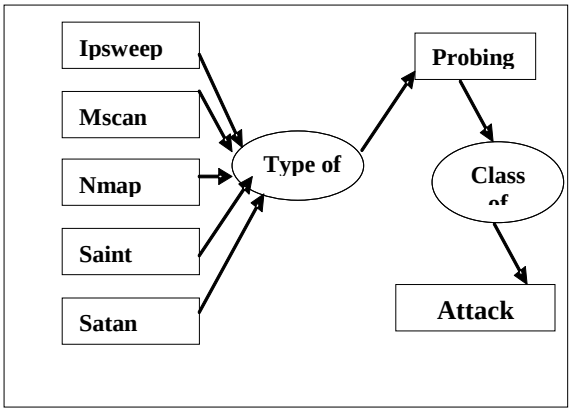

Figure 4: Conceptual graph used in Intrusion Class Recognition

B. Fuzzy Cognitive Map Intrusion Diagnosis Layer

In this paper, we consider conceptual graph as an appropriate contextual tool to know context (limits or boundaries) of intrusion effect on target system. This is done due to classification function of conceptual graph. If intrusion class is well known it will be easy to know which intrusion target system components are influenced by intrusion effect. We use Fuzzy Cognitive map in this purpose.

1) Fuzzy Cognitive Map

A Professor from the University of Southern California, Bart Kosko, introduced Fuzzy cognitive maps (FCM) in 1986 as an extension of cognitive maps [10]. Earlier in 1948, Tolman presented the key concept of the "cognitive maps" to describe complex topological memorizing behaviors in the rats [35]. In the Seventies, Axelrod described the "cognitive maps" in the shape of directed, interconnected, bilevel-valued graphs, and used them in decision theory applied to the politico-economic field [34].

FCMs are a soft computing method for simulation and analysis of complex system and originally applied to problems concerning political science [36]. Kosko proposed the idea of FCMs that are signed directed graphs for capturing causal knowledge and processing computational inference [17,18,19]. FCMs model the world as concepts and causal relations between concepts in a structured collection. Concepts (nodes) in an FCM are events that originate in the system and whose values change over time. Concepts take values in the interval [0,1]. The causality links between nodes are represented by directed edges that measure how much one concept impacts the other(s) [27].

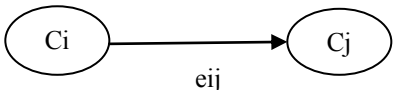

Figure 5: Two FCM concepts and a connecting edge representing a causal link

As shown in Figure 2, the edge value between concept Ci and Cj can be represented by eij. The weight associated with an edge takes values in the interval [-1, 1]. An edge value of eij =0 indicates that there is no relation between the concepts Ci and Cj. A value eij>0 denotes positive causality— whenever concept Ci increases, Cj increases by the degree eij.

Conversely, eij<0 denotes negative causality— whenever concept Ci increases, there is a decrease in Cj by the degree eij. The higher the absolute value for eij, the greater the effect of the cause. FCMs can be successfully used to capture causal knowledge and to support causal inference[21]. A FCM graph can be equivalently defined by a square matrix, called connection matrix, which stores all weight values for edges between corresponding concepts represented by rows and columns. The system of n nodes can be represented by n×n connection matrix [36]. An example of FCM model and its connection matrix are shown as follow:

$$\begin{bmatrix} e11 & e12 & e13 \\ 0 & 0 & e23 \\ e31 & 0 & 0 \end{bmatrix}$$

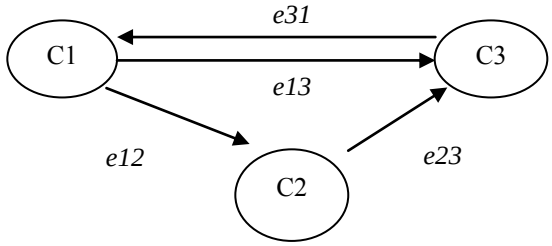

Figure 6: A simple fuzzy Cognitive Map

Where, weight eij specifies the value of an edge from i^{th} to j^{th} concept node. The value of the weight *eij* specifies how strongly the causal concept *Cj* affects the effect concept *Ci*. While a positive value of e*ij* represents a proportional effect, a negative value represents an inversely proportional effect and zero e*ij* represents the absence of an effect.

The inference mechanism of FCM is described by the following formula:

$$\begin{cases} S(t) = (si(t))1XN & i,j = 1,2,\dots,N, \\ si(t+1) = f\left(\sum_{j=1}^{N} si(t)Xeij\right) & t = 0,1,2,\dots,T. \end{cases}$$

Where t is the iteration step, and $si(t)$ indicates the state value of concept Ci at iteration t. $S(t)$ indicates the system state at iteration, and f is a threshold function [36].

2) Intrusion Victim System Diagnosis

Several pieces of information are necessary in order to plan a sequence of response actions. For the system we are protecting, we need a clear representation of the most valuable resources and also the underlying resources that provide the basic functionality. The true value of some resources (for example, the TCP/IP network service) is heavily influenced by other resources that depend on them (network is needed by *httpd*, etc.), and we need a clear way to reflect these dependencies before we can decide how to deal with a compromised entity that give us the basis for deciding on response strategy [3].

Intrusion consequence on victim computer system can differ from one computer component to another. If a computer system component is victim of intrusion, neighboring computer system component can be influenced by negative effect of intrusion on the former. The influence is depending on the correlation that can exist between two components.

Ivean Balepinet et al. developed a system map which represents dependencies between the resources. If an edge is directed from node A to node B, it means that A provides some service to B, B depends on A, and, most likely, A produces information that B consumes [3].

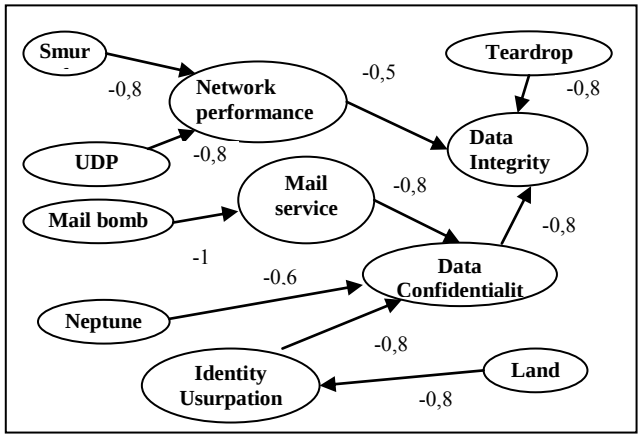

Figure 7: Fuzzy cognitive map of mutual intrusion negative influences .

In this paper, we developed a fuzzy cognitive map which represents influences between computer system components or security concepts related to intrusion detected, where nodes represent computer system components or security concepts and arcs represent mutual influences between two nodes as consequent of damage caused by intrusion. Influences between nodes of this map are evaluated as a fuzzy negative degree positioned between 0 and -1. When fuzzy degree is near of -1 then it is considered as very high negative influence, however there is a poor negative influence when this degree is near of zero. A +1 influence degree means strong effect between concepts.

C. Agent Response Layer

Intelligent agents represent a recent approach that proves its usefulness in security field. They are mainly used in intrusion detection system for enhancing the detection capability in distributed environment. Recent works are interested in using these agents to provide automated responses, as mentioned in the following models [11].

Adaptive Intrusion Response using Attack Graphs in E-Commerce Environment (ADEPTS): it is an autonomous intrusion tolerant system that includes an automated response mechanism to counter the detected attacks. It aims to monitor and track intrusions as they occur in real time, and deploys various wide ranging responses to contain and restrict the propagation and escalation of attacks in the system.

Event Monitoring Enabling Responses to Anomalous Live Disturbances (EMERALD): it is a cooperative and distributed hybrid intrusion detection and response system that consists of hierarchical collections of monitors. Adaptive Agent-based Intrusion Response System (AAIRS): it is considered as an extension of the EMERALD model, incorporating more complete response taxonomy and an adaptive response mechanism that uses additional criteria in formulating an appropriate response.

Automated Response Broker (ARB): it is a host based intrusion detection system that couples automated response with specification-based. It is based on a system map and a cost model for its response selection process. It operates even in the presence of uncertainty.

Automatic Response Systems are systems which provide immediate response to the detected intrusion through an automated decision making process. In this case, a decision making tool, that includes a set of predefined actions, plays the role of a system administrator and triggers response(s) automatically when detecting appropriate intrusion.

The main strength of these systems compared with the others lies in the decrease of time delay, close to zero. However, the development of an intelligent computer

decision tools that mimic human to respond appropriately and correctly to intrusions is still unavailable [1,10,11, 32].

The third layer of our Fuzzy Contextual Cognitive Intrusion Response System is an effective response multiagent system where an agent can be responsible of solving the damage caused by an intrusion on computer system components. Agents are organized by intrusion classes: DOS, PROBING, U2R and R2U. For each intrusion class, we specify two types of agents: specialized agent and mobile agent.

Specialized agents use information coming up from diagnosis layer in order to specify suitable remedies. They check the cure process of victim system by notifying system administrator and/or acting directly on the victim system by means of mobile agents.

The developed prototype of this system can accomplish two functions: automated response or no. For automated intrusion response function, agent can only send notification message to intrusion victim system administrator in which it explains the corrective tasks to be done by him, however in case of automated intrusion response system, mobile agents will be charged by those corrective tasks rather than system administrator.

VI. CONCLUSION

This research work make up a new framework of intrusion response system based up on two features: the class of intrusion which is named context and the victim system map. The latter shows influences between computer/system components and security concepts and it's built using fuzzy cognitive map. However, the former point out the nature/class of intrusion which can be used to easy conduct victim system diagnosis and find convenient remedies.

Implementation of this intrusion response system prototype was done using Java Language and Jade multiagent platform. First results seems to be encouraging and we have to progress in deeply testing process in order to evaluate system efficiency when providing remedies to victim system. In fact, this response system will be integrated as a third layer to an intrusion detection and prevention system that we developed its two first layers: detection and prediction layers in one of our previous papers [14].

Future research work that we think conduct as an extension of this paper concerns intrusion response system learning module which will allow response system to remember old remedies (solutions) and adopt them depending on similarity between attacks.

ACKNOWLEDGMENT

This project was supported by the deanship of scientific research at Salman bin Abdulaziz University under # 33/ت/78, KSA.

REFERENCES

[1] Anuar N.B., Papadaki M., Furnell S.M., Clarke N.L.: An investigation and survey of response options for Intrusion Response Systems (IRSs) Proceedings of the 9th Annual Information Security South Africa Conference, Sandton, South Africa, 2 - 4 August, pp1-8, ISBN: 978-1-4244-5493-8, (2010)

[2] Arfaoui N., Jemili F., Zaghdoud M., Ben Ahmed M.: Comparative Study Between Bayesian Network And Possibilistic Network in Intrusion Detection », In Proc. of the International Conference on Security and Cryptography, Secrypt, Portugal (2006).

[3] Ivan B., Sergei M., Jeff R., and Karl L.: Using Specification-Based Intrusion Detection for Automated Response. International symposium on recent advances in intrusion detection N°6, Pittsburgh PA , USA: September 08, 2003 , vol. 2820, pp. 136-154 (2003).

[4] Baudrit C. and Dubois D. : Représentation et propagation de connaissances imprécises et incertaines: Application à l'évaluation des risques liées aux sites et aux sols pollués. Université Toulouse III – Paul Sabatier, Toulouse, France, Mars (2006).

[5] Bauer D. S. and Koblentz M. E.: NIDX: An Expert System for Real-Time Network Intrusion Detection," Proceedings of the Computer Networking Symposium, pp. 90-106, Washington, DC, April (1998).

[6] Boonthum C., Toida S. and Levinstein I. B.: Paraphrasing Recognition through Conceptual Graph, Department of Computer Science, Old Dominion Universiy, Norfolk, Virginia, USA, (2003)

[7] Cuppens F. and Ortalo R.: LAMBDA: A language to model a database for detection of attacks. In Third International Workshop on the Recent Advances in Intrusion Detection (RAID'2000), Toulouse, France, (2000).

[8] DARPA. Knowledge Discovery in Databases, 1999. DARPA archive. Task Description http://www.kdd.ics.uci.edu/databases/kddcup99/task.htm Accessed October 10, (2007)

[9] DARPA Cyber Panel Program. DARPA cyber panel program grand challenge problem (GCP). http://www.grandchallengeproblem.net/, Accessed October 10, (2007).

[10] Eng, P., Haug, M.: Automatic Response to Intrusion Detection. Faculty of Engineering and Science, Agder University College, June (2004).

[11] Fessi B. A., Hamdi M., Benabdallah S., Boudriga N.: Automated Intrusion Response System: Surveys and Analysis. In Proceedings of Security and Management'2008. pp.149-155, (2008).

[12] Gruber T.: Ontology, *Encyclopedia of Database Systems.* Ling Liu and M. Tamer Özsu (Eds.), Springer-Verlag, (2008).

[13] Hayes, P. J.: The Second Naïve Physics Manifesto. Hobbs and Moore (eds.), *Formal Theories of the Common-Sense World*, Norwood: Ablex, (1985).

[14] Jemili F., Zaghdoud M., Benahmed M.: HIDPAS: Hybrid Intrusion Detection and Prediction multiAgent System. *International Journal of Computer Science and Information Security, Vol. 5, No.1, (2009).*

[15] Jemili F., Zaghdoud M., Ben Ahmed M.: Intrusion Detection based on Hybrid Propagation in Bayesian Networks. In Proc. of the IEEE International Conference on Intelligence and security informatics, ISI (2009).

[16] Jemili F., Zaghdoud M., Ben Ahmed M.: Attack Prediction based on Hybrid Propagation in Bayesian Networks. In Proc. of the Internet Technology And Secured Transactions Conference, ICITST (2009).

[17] Kosko, B.: Fuzzy cognitive maps. *International Journal of Man-Machine Studies.*1986 (24) pp: 65-75 (1986).

[18] Kosko, B.: *Neural networks and fuzzy systems: A dynamical systems approach tomachine intelligence.* Englewood Cliffs, NJ: Prentice Hall.(1992).

[19] Kosko, B.: *Fuzzy engineering.* Upper Saddle River, NJ: Prentice Hall.(1997).

[20] Kruegel C., Darren M. W., Robertson F. V. : Bayesian Event Classification for Intrusion Detection Reliable Software Group. University of California, Santa Barbara, (2003).

[21] Lee, K. C. and Kim H. S.: A causal knowledge driven inference engine for expert system. In *Proceedings of the annual Hawaii international conference on system science*. pp: 284- 293 (1998).

[22] Mukherjee B., Heberlein T. L. and Levitt K. N.: Network intrusion detection. IEEE Network. 8(3):26{41, May/June (1994).

[23] Onashoga S. A., Akinde A. D., and Sodiya A. S.: A Strategic Review of Existing Mobile Agent-Based Intrusion Detection Systems. Issues in Informing Science and Information Technology Volume 6, (2009).

[24] Rash M. et al.: Snort 2.1 Intrusion Detection, Chapter 12: Acrive Response, pp 605-670, Second edition, Syngress Publishing, (2004).

[25] Scarfon C., Mell P.: Guide of Intrusion Detection and Prevention System. National Institute of Standard and Tachnologies, NIST, Special Publication, 800-04, February (2007).

[26] Sebring M. M. et al.: Expert Systems in Intrusion Detection: A Case Study. Proceedings, 11th National Computer Security Conference, pp. 74-81, October (1988).

[27] Siraj A., Bridges S. M. and Vaughn R. B.: Fuzzy Cognitive Maps for Decision Support in an Intelligent Intrusion System. Department of Computer Science Mississippi State University Misstate, MS 39762, (2000).

[28] Smaha S. E.: Haystack: An Intrusion Detection System. Fourth Aerospace Computer Security Applications Conference, Orlando Florida, pp. 37-44, December (1988).

[29] Sowa J. F.: *Conceptual Structures: information Processing in Mind and Machine*. Addison- Wesley, MA (1983).

[30] Sowa, J. F.: *Conceptual Structures. Information Processing in Mind and Machine,* Reading, MA: Addison Wesley, (1984).

[31] Sowa, J. F.: Conceptual Graphs as a Universal Knowledge Representation. *Computers Math. Application*, 23(2-5): pp:75-93 (1992).

[32] Stakhanova, N., Basu, S., Wong, J.: Taxonomy of Intrusion Response Systems. International Journal of Information and Computer Security, Vol. 1, No. 1, (2006).

[33] Stakhanova N., Basu S., Wong J.: A Taxonomy of Intrusion Response Systems. International Journal of Information and Computer Security, Volume 1, Issue ½, Jannuary (2007).

[34] Tarantola C.: Ontology Engineering by Fuzzy Cognitive Maps. National Conference on Radio communications and Broadcasting, KKRRiT, VISNET, Warsaw, 16-18 June (2004).

[35] Tolman E.C., "Cognitive Maps in Rats and Men", Psychological Review, 42, 55, pp: 189-208, (1948).

[36] Wang a.b H., Wang a.b Li, Application of Improved Fuzzy Cognitive Map Based on Fuzzy Neural Network in Intrusion Detection, Journal of Information & Computational Science 10: 1 (2013) 271–278, Available at http://www.joics.com.

[37] Yue H., Chun-Mei L.: Partitioning Study of Complex System, WSEAS TRANSACTIONS on SYSTEMS, Issue 12, Volume 7, ISSN: 1109-2777, December (2008).