2009 IEEE/WIC/ACM International Joint Conference on Web Intelligence and Intelligent Agent Technology

Agent-based Security System for User Verification

Erik Dovgan, Boštjan Kaluža, Tea Tušar, and Matjaž Gams
Department of Intelligent Systems
Jožef Stefan Institute
Jamova cesta 39, 1000 Ljubljana, Slovenia
{erik.dovgan, bostjan.kaluza, tea.tusar, matjaz.gams}@ijs.si

***Abstract*—We present a security system consisting of an arbitrary number of entries, sensors and agents. The intelligent integrated system is based on user modeling, i.e. models of their previous entries, using several levels of description and several single machine learning agents. The system is specialized for high-security tasks, e.g. controlling entry to a headquarter and for scenarios including terrorist attacks or kidnapping, when the attackers formally bypass the existing sensors, but fail to imitate normal movement of an employee. An experimental setup was implemented to verify the successfulness of the approach.**

Agents, security system, access control

I. INTRODUCTION

Access control prevents unauthorized persons to access secure areas, documents, buildings and services. It usually consists of an identification stage, where users introduce themselves to the system, and a verification stage used to ensure that introduced users' identity is valid. If the identity of the user is approved, then the user may access secure area with the assigned permissions. This access schema is used in several variations, for example, logging on ATM machines, e-banking accounts or for physical security of a room or building.

This paper presents an intelligent agent system that upgrades access control by providing an additional security layer. The proposed system acquires additional knowledge from previous experiences by constructing user behavior models [1]. It is capable to detect abnormal behavior of users and display an alarm with an explanation. A basic version of the system without ontology and agents was presented in [2].

By constructing user models, the security system improves "thinking and awareness" of the environment with several artificial intelligence (AI) agents based on knowledge stored in the form of an ontology [3]. The intelligence was added to the classical entry system in order to increase security by new functionality.

The paper is organized as follows. Section 2 describes the related work. Section 3 presents a general architecture of the proposed security system with the accompanying ontology. An experimental environment and agents are described in Section 4. Section 5 presents the experiments. Section 6 summarizes the work done and concludes with a discussion.

II. RELATED WORK

Modern behavior analysis is often based on past users' behavior. Hilas and Mastorocostas [4] investigated different learning approaches for preventing telecommunication frauds. They built user behavior models and detected frauds. Adeva and Atxa [5] introduced intrusion detection based on text-mining techniques.

Video surveillance methods are often used for detection of unusual behavior. Wilson [6] presented an intelligent system, which adds data mining methods to the existing system of cameras in a building. Sun and Tien [7] proposed an approach for recognizing human facial emotions in order to further detect human suspicious behaviors.

Modern control typically uses several sensors, e.g., biometric sensors, a speech sensor or a touch sensor. Wahyudi and Syazilawati [8] described an intelligent access control system with speech analyses used for person verification. Lambort and Williams [9] introduced an intelligent system which consists of several heterogeneous sensors with a weighted voting algorithm for computing the final result.

In summary, the presented approaches use several intelligent methods, but each approach focuses on only one, the most promising method. Besides, knowledge is stored in a method-appropriate way; therefore, it is not commonly accessible and cannot be used by other agents for further data analysis. This paper proposes a new approach for behavior analysis and intrusion detection. It uses several intrusion detection classification techniques realized as agents. The knowledge is stored in a common ontology which enables interchangeability of knowledge between agents. Consequently, additional agents or applications can be easily added to the system.

III. SECURITY SYSTEM ARCHITECTURE

In this section, system architecture and ontology are presented.

A. The system architecture

The proposed system consists of three main hardware components: access points, sensors and a network. Sensors provide data when a user produces an event. The data is sent through a network to the ontology. The ontology is used as a communication channel between agents.

In the proposed security system, an arbitrary number of sensors can be applied. Commonly used sensors provide

978-0-7695-3801-3/09 $26.00 © 2009 IEEE
DOI 10.1109/WI-IAT.2009.295

information about a person's identity card, fingerprint, face, cornea, etc. In the system there can also be an arbitrary number of intelligent agents, integrated into one classifying system. Each agent monitors data in the ontology and reacts if relevant patterns appear. Furthermore, each agent sends the classification result to the ontology. An agent can also trigger an action regarding to the classification result, e.g., show the result on the screen, prevent user entry, or produce an alarm. The top agent is the integrating agent, providing a final decision about the entry.

B. Ontology

The communication and integration between agents are done indirectly through the ontology. Agents' knowledge is also stored in the ontology and can be easily accessed by other agents as shown in Figure 1. All classification agents can read and write to the common knowledge, therefore, they can also use other agents' classifications. As a result, several layers of learning potentially appear: basic learning, meta-learning, meta-meta-learning etc. As described later, the experimental set-up uses three layers.

The presented messages and data are stored in Web Ontology Language (OWL) [3], a standard language for describing classes or entities, properties, relations between classes, rich types of properties, cardinality of properties, and characteristics of properties.

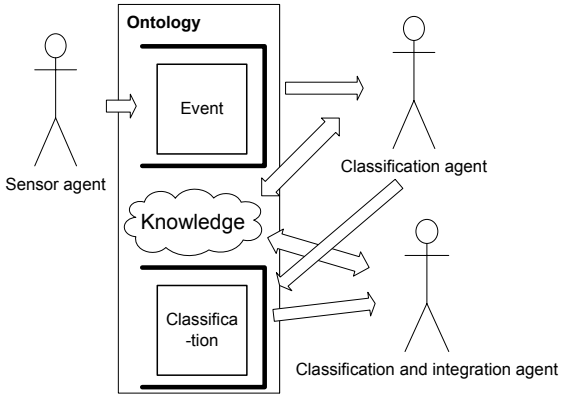

Figure 1. Communication between agents through the ontology

IV. AN EXPERIMENTAL SETUP

To verify the approach, an experimental system was designed, consisting of several hardware and software components.

A. Experimental configuration

The proposed system schema does not restrict the number of sensors and their variety, but a specific configuration has to be chosen for empirical tests. The constructed environment consisted of a single access point with a door equipped with an open/close door sensor, an identification card reader, a fingerprint reader, and a camera. If the classification agents confirm the entry, the door unlocks and the user can pass through.

For each entry, the event data are processed and classified by agents. The integration agent calculates the final classification. Each agent can classify an event into one of the following three categories: OK, Warning, or Alarm. It also provides detailed explanation of its decision, comprehensible to the supervisor.

B. Agents

The experimental system consists of four groups of classification agents, namely reflex agents, micro learning agents, macro learning agents and visual learning agents, and one integration agent as shown in Figure 2. In the next sections, the agents are described in more details.

1) Reflex agents: The reflex agents implement rules and do not learn from the past events. They are realized as generic reflex agents and become operable when their parameter values are defined. The final classification is an alarm as soon as one reflex agent classifies the entry as an alarm. In the experimental system, the following generic reflex agents were implemented and parameterized: macro time agent, micro time agent, macro event sequence agent and micro event sequence agent. From these 4 generic agents, 10 executable reflex agents were generated.

2) Micro learning agent: The micro learning agent has been designed based on empirical evidence that users' entry in their own personalized manner and rarely change their habits over time, e.g., a female user usually carries her card in a handbag.

The users' habits are modeled as follows. All event data consist of four micro times: ID card time, fingerprint time, door opening time and door closing time. Three time differences are calculated between successive micro times. These differences determine a 3-dimensional micro features space. Therefore, every user's enter represents a point in the space. If a new entry is close to the regular entries cluster of the entering identified user, then the user is considered entering normally. We experimented with several algorithms for outlier detection and finally LOF (Local Outlier Factor) was chosen [10]. Therefore, although several agents were tested, only one was finally implemented.

3) Macro learning agents: The macro learning agents are focused on daily routine of the users passing through one access point, and movements between different access points. E.g., some users usually come to work together; some are smokers and pass through a particular access point more often. To detect such routines and dependencies between users, the following macro features were used: time, date, day of the week, date in relation to the month, etc.

The top macro agent is an integration second-layer agent, which combines the results of three single macro agents. The first and the second macro agents apply the C4.5 algorithm [11] for constructing decision trees. The first agent uses only macro features of the entry, while the second agent uses both macro and micro features. Therefore, it joins the macro knowledge with the micro learning module knowledge, using the ontology. The third agent uses the LOF algorithm on

macro and micro features. It also joins macro knowledge and micro learning module knowledge, saved in the ontology. The final classification by the top macro integration agent was first obtained by voting and later by more complex algorithms.

4) Visual learning agent: The visual learning agent uses the body movement of each person for his/her identity verification. As the micro learning agent, the visual agent also takes into consideration that users move in their own personalized manner, which rarely changes.

A user is verified by extracting the movement signature from the entry video. The signature is obtained with the identification of elementary movements, estimated with histograms. Then it is compared with user's past movement signatures. If the similarity is high, the user is positively verified. A detailed explanation of the method is in [12].

5) Integration agent: This third-level agent combines the results from previous described agents as follows. When the reflex agents report an alarm, all the other agents are not relevant as something is very wrong and demands urgent action. Therefore, the reflex agents trigger an alarm and the integration agent is just informed. However, in most of the entries classification agents asynchronously classify in two iterations. The integration agent observes classifications of other agents and provides current decisions. After a certain time or when all classification agents classify, the integration agent provides the final decision. An alarm can be triggered any time during classifications.

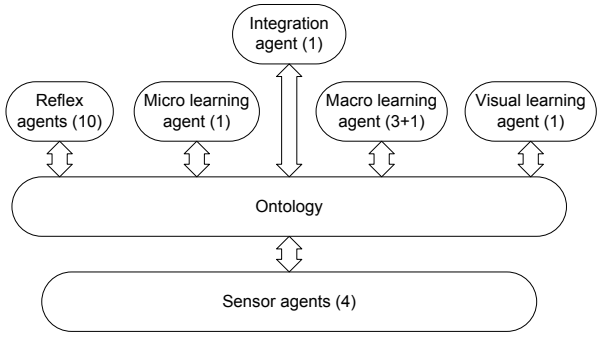

Figure 2. Agents in the experimental setup

V. EXPERIMENTAL RESULTS

We used an experimental environment as described in Section 4.1. Entries were produced by five employees, each performing 40 regular entries. Next, the fake-identity experiment was simulated by testing each employee's entries on other employees' entries. The offline simulation with visual learning agent is hard to perform, thus we tested the events only with reflex agents, micro learning agents and macro learning agents.

Table 1 shows the results for simulation of 200 regular entries of 5 employees. The system correctly classified 88% of such entries. Table 2 shows the results for simulation of 200 fake-identity entries of 5 employees, when a user forged another ID, but retained the movement. The system correctly classified 69% of such events. This table also shows that the reflex agents classified all fake-identity entries as regular entries. This occurs because reflex agents check only the entry regularity and do not classify an entry based on a user's behavior.

TABLE I. RESULTS FOR REGULAR ENTRIES

Agents	Reflex	Micro learning	Macro learning	Integrati-on
OK	100%	98%	90%	88%
Warning	0%	2%	10%	12%
Alarm	0%	0%	0%	0%

TABLE II. RESULTS FOR FAKE-IDENTITY ENTRIES

Agents	Reflex	Micro learning	Macro learning	Integrati-on
OK	100%	35%	14%	13%
Warning	0%	15%	24%	18%
Alarm	0%	50%	62%	69%

It must be emphasized that the tests were made as if the biometric control was trivially by-passed. In real life, the biometric control is the basic security control, hard to overcome on its own. The intelligent agents represent an additional level of security for high-security areas.

VI. CONCLUSION AND DISCUSSION

A security agent system for access control is presented, based on an arbitrary number of sensors, entries and intelligent agents communicating through the system ontology as message and knowledge storage. It is specialized for high-security applications in scenarios when existing sensor-based access control is by-passed. The system learns employees' movement and checks new entries on this basis. The system uses an ontology and agents, thus enabling quick adaptation to any particular application.

Experimental verification was performed with a fake-identity experiment. The experimental system successfully recognized 88% of the regular entries and 69% of the fake-identity entries. Experiments indicate that applying the proposed security system on top of existing access systems might substantially improve security. A drawback of the proposed system is additional time, needed for learning behavior of the users. The system becomes fully operational only after a certain number of entries. Finally, such advanced security might be more of a nuance than an asset for non-security applications. Several modifications are needed for other types of applications, e.g., e-banking.

In our experience, the major advantage of our approach is in several agents using various methods and various viewpoints and flexible interchange of information stored in the ontology.

REFERENCES

[1] C. Ramos, J. C. Augusto and D. Shapiro, "Ambient Intelligence – the Next Step for Artificial Intelligence", *J. Intelligent Systems*, 2008, pp. 15-18.

[2] M. Gams and T. Tušar, "Intelligent High-Security Access Control", *Informatica*, vol. 31, no. 4, Slovene Society Informatika, 2007, pp. 469-477.

[3] K. Breitman, M. Casanova and W. Truszkowski, *Semantic Web: Concepts, Technologies and Applications*, Springer, London, 2007.

[4] C. S. Hilas and P. A. Mastorocostas, "An application of supervised and unsupervised learning approaches to telecommunications fraud detection", *Knowledge-Based Systems*, vol. 21, Elsevier, 2008, pp. 721-726.

[5] J. J. G. Adeva and J. M. P. Atxa, "Intrusion detection in web applications using text mining", *Engineering Applications of Artificial Intelligence*, vol. 20, Elsevier, 2007, pp. 555–566.

[6] D. L. Wilson, "Intelligent video systems for perimeter and secured entry access control", *Proceedings of the 39th Annual IEEE International Carnahan Conference on Security Technology ICCST*, IEEE, 2005, pp. 260-262.

[7] T.-H. Sun and F.-C. Tien, "Using backpropagation neural network for face recognition with 2D + 3D hybrid information", *Expert Systems with Applications*, vol. 35, Elsevier, 2008, pp. 361-372.

[8] W. A. Wahyudi, and M. Syazilawati, "Intelligent Voice-Based Door Access Control System Using Adaptive-Network-based Fuzzy Inference Systems (ANFIS) for Building Security", *Journal of Computer Science* 3, 2007, pp. 274-280.

[9] P. Lamborn and P. J. Williams, "Data fusion on a distributed heterogeneous sensor network", *Proceedings of SPIE - The International Society for Optical Engineering*, vol. 6242, Bellingham, Washington, 2006, pp. 1-8.

[10] M. M. Breunig, H. P. Kriegel and J. Sander, "LOF: Identifying density-based local outliers", *Proceedings of the International Conference on Management of Data SIGMOD'00*, 2000, pp. 93–104.

[11] J. R. Quinlan, *C4.5: Programs for Machine Learning*, Morgan Kaufmann, 1993.

[12] J. Perš, M. Kristan, M. Perše and S. Kovačič, "Motion based human identification using histograms of optical flow", *Proceedings of the 12th Computer Vision Winter Workshop CVWW*, Graz University of Technology, 2007, pp. 19-26.