Paper

Simulation Model of Biometric Authentication Using Multiagent Approach

Adrian Kapczyński and Tomasz Owczarek

Institute of Economics and Informatics, Silesian University of Technology, Zabrze, Poland

Abstract—In this article authors present the concept of application of multiagent approach in modeling biometric authentication systems. After short introduction, we present a short primer to multiagent technology. Next, we depict current state of the art related to biometrics combined with multiagent approach. In the next part of the work we present four exemplary simulation models of biometric authentication environments as well as the results of their examination.

Keywords*—*biometrics, multiagent, multimodal, simulation.

1. Introduction

Current level of requirements related to strong authentication mechanisms are either fulfilled by constructing single, strong authentication factor solution or a solution that utilizes the multifactor approach. Analogically, in case of user verification or identification, biometric methods are widely applied as single modal or multimodal systems. Contemporary theoretical and empirical approaches to construct biometric systems focus on converging different authentication factors, algorithms, protocols and equipment in networked environments. This emphasize the emerging role of methods and tools used to model, simulate and analyze networked and more complex then single instance systems. Therefore, the need of performing analysis from different abstraction levels systems can be satisfied by providing apparatus operating not only from micro, but also macro perspective. Complete biometric system models shall combine technical and non-technical (human) element. Such approach can be found in many modeling languages, even in BANTAM (biometric and token modeling language) language, dedicated to biometric domain. BANTAM however does not provide the capability of observing the active, environment of biometric systems. In this article authors propose the use of multiagent systems as simulation tools of biometric authentication systems. The authentication processes are realized between users (agents having the need of being authenticated) and the authentication center. This concept we illustrate by four simulation models of single- and multibiometric authentication environments. In next part of the work we present a primer on multiagent systems.

2. Multiagent Systems

Agent-based model can be simply defined as a simulation made up of agents, objects or entities that behave autonomously [1]. The shortest definition of the term agent can be found in [2], where it is described as a proactive object. These two definitions contains two main features of agency:

- proactiveness: agent can take initiative, it does not simply wait for a signal to start acting but it is able to undertake actions in order to fulfill its goals;
- autonomy: agent is an autonomous entity which can operate without direct control.

Apart from these Wooldridge and Jennings [3] provide two more essential agents' properties:

- reactivity: agents respond to signals perceived from their environment;
- social ability: agents interact with each other, they communicate, cooperate and even compete.

According to [4] the indispensable feature of any agent is its (temporally) continuity which means that it is a continuously running process. Franklin and Graesser also propose a taxonomy of agents which at the highest level divides them into biological agents (human and animal), robotic agents and computational agent (computer program). Agent's definition varies and different features are emphasized depending on authors [5], [6]. But they all agree that an agent is situated in some environment and able to make autonomous decisions [7].

As it is pointed out in [6], [4], [8] one cannot talk about agent without environment in which it is situated. According to the definition from [5] an agent is "anything that can be viewed as perceiving its environment through sensors and acting upon the environment through actuators". A schema of an agent interaction with its environment is shown in Fig. 1.

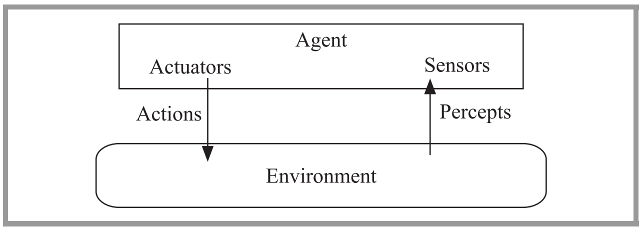


Fig. 1. Agent and its interaction with environment.

The environment determines an agent; placing an agent in a different environment often stops it from being an agent (e.g., a robot with only visual sensors placed in a dark room) [4]. Single agent environment are very rare. In fact, in multiagent systems community exists a popular slogan that "there's no such thing as a single agent system" [6, pp. 105]. Complexity and unpredictability of real world situations often require a combination of specialized problem solvers (agents) which cooperate in order to find a solution to problems that are far beyond their individual capabilities [9]. When there are more than one agent then we deal with multiagent system and agent's environment is constituted by all other agents. Agent-based models are useful in modeling complex, nonlinear systems. But they can be also treated as generalizations of analytical models [10], especially when the system modeled consists of numerous interacting autonomous objects. This is why we chose agent-based approach to the specified problem. In next part of the work we present the current approaches in combing biometrics with multiagent methodology.

3. State of the Art

M. Abreu and M. Fairhurst [11] focus on evaluation of multimodal structures and they investigate how fundamentally different strategies for implementation can influence the degree of choice available in meeting chosen performance criteria. In particular they implement computational architecture based on a multiagent approach which goal is to achieve high performance. In their work authors also propose and evaluate a novel approach to implementation of a multimodal system based on negotiating agents.

R. Meshulam et al. [12] introduced the concept of multiagent framework which works in large-scale scenarios and is capable of providing response in real time. The input for the framework is biometric data acquired at a set of locations and that data is used to point out individuals who act accordingly to pattern defined as "suspicious". Authors present two interesting scenarios in order to demonstrate the usefulness of their framework. In first scenario, the goal of the system is to point to individuals who visited a sequence of airports. In this scenario, face biometrics is applied. The goal in the second scenario is to point out individuals who called a set of phones. In the second scenario the use of speaker biometrics is proposed.

G. Ali, N. Shaikh and Z. Shaikh note that traditional insider threat protection models are not efficient and that there is a need of an autonomous and flexible model against insider threat [13]. In the paper authors present agent-based model that monitors behavior of the authorized users. So, the agents are responsible for recording all actions of the authorized user and deliver all recorded data to the main agent for processing and decision making.

Finally, G. Chetty and D. Sharma present an application of agent technology to the problem of face identification, which is performed robustly in even difficult environmental conditions [14]. Authors apply new composite model consisting of multiple layers that is supported by integration with agent based paradigm. Obtained experimental results are suggesting further investigations in application of agent methodology in building multimodal biometric systems. Other similar approaches can be found in [15], [16].

We can notice that agent-based concept is applied in order to enhance the performance of single instance (but not only single modal) biometric systems or to provide capabilities of detection of inexpedient behavior from security point of view. In this work we proposed complementary approach which relies on use of agent-based paradigm for simulation enabling macro scale analysis of interactions between authenticator and authenticatee. In next part of the paper we present the foundation of agent-based biometric authentication as well as we illustrate it by providing three examples.

4. Agent-Based Biometric Authentication

Our models were created in NetLogo, a multiagent programmable modeling environment [17]. This allowed for rapidly implementation of the model's variants and made all results scientifically reproducible. There are three types of agents in proposed model: users, authentication centers, and experts (Fig. 2).

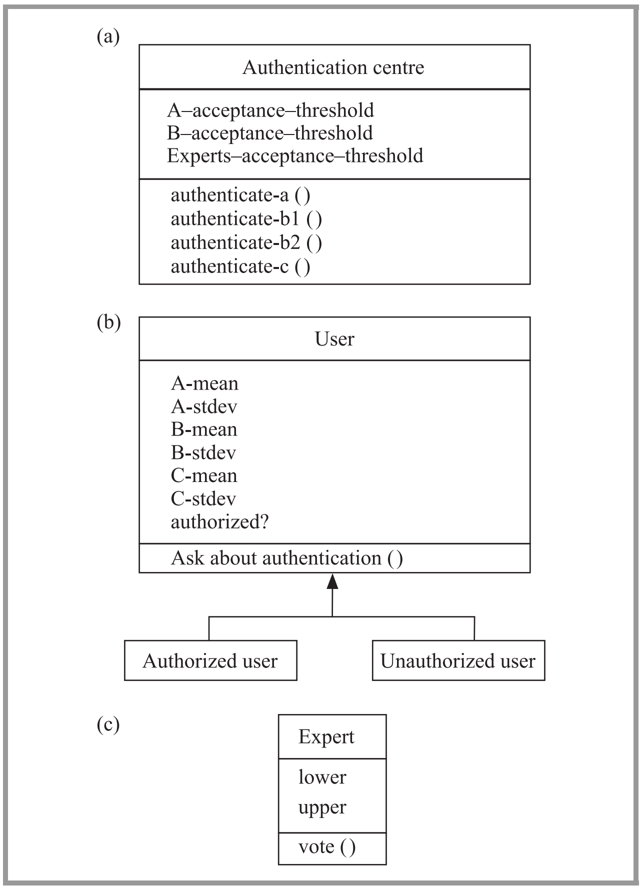


Fig. 2. Agent types: (a) authentication centre, (b) user, (c) expert.

Users (agents being authenticated) are divided into genuine users (authorized) and impostors (unauthorized). Distinction between those agents is performed by use of attribute

`Authorized?` (taking values true or false). Each user has three modalities: A, B and C. Those biometric characteristics are here represented by matching scores, which are an output of comparison module performing action on enrollment and verification templates. The enrollment template is created during the first interaction with biometric system and arises from raw biometric data which is transformed into its mathematical representation. The reference template is created every time the user wants to be authenticated basing on provided raw biometric data. Each agent has for each modality one corresponding matching score described using two attributes: the average and standard deviation. Matching scores are random variables with normal distribution. In addition to the operations shown in Fig. 2 `ask about authentication()`, all users have the instructions also responsible for their movement to and from the authentication center (they are not relevant to the described problem). Authentication centers have attributes which are acceptance thresholds and operation `authenticate()`. The experts occur only in third variant of simulation models. Description of their attributes are presented in further part of this article.

Overall, the simulation process is as follows. After the opening initialization of agents (users stay in randomly deployed in a two-dimensional space, inside which there is a authentication center), any user at random intervals goes to the authentication center. Upon arrival agent delivers its matching score (for each modality the system generate a random value of a random variable). On that basis the center formulates decision: accept or reject. Regardless of the result, the user returns to its initial position and looks forward to the next signal of going to the authentication center.

Basing on formulated above general foundings, four simulation models of biometric authentication systems were constructed.

Model a. Multiagent system with given number of authorized and not-authorized agents and with one authentication centre. The authentication centre during authentication process receives from the authenticated agent its matching score of modality A which is compared to global threshold TA. The output of the comparison is the basis of the decision about acceptance (in case the matching score is equal or grater than threshold) or rejection (in case the matching score is lesser than threshold).

Model b1. Multiagent system with given number of authorized and not-authorized agents and with one authentication centre. The authentication centre during authentication process receives from the authenticated agent its matching score of two modalities: A and B. The matching scores are compared with appropriate global thresholds TA and TB respectively. The outputs of performed comparisons are the basis of the final decision. The system accepts the users if both matching scores are not lesser than given thresholds (AND rule) else it rejects the user.

Model b2. Multiagent system with given number of authorized and not-authorized agents and with one authentication centre. The authentication centre during authentication process receives from the authenticated agent its matching scores of two modalities: A and B. The matching scores are compared with appropriate global thresholds TA and TB respectively. The outputs of performed comparisons are the basis of the final decision. The system accepts the users if at least one matching score is not lesser than given threshold (OR rule) else it rejects the user.

Model c. Multiagent system with given number of authorized and not-authorized agents and with one authentication centre. The authentication centre during authentication process receives from the authenticated agent its matching scores of three modalities: A, B and C. The authentication process is carried out by three experts and each expert has its own set of two thresholds (upper limit and lower limit). If matching score is greater or equal than upper limit than user is accepted else if matching score is lesser or equal than lower limit then user is rejected else the decision is inconclusive. Experts has predefined set of thresholds (presented as s triple: expert number, upper limit, lower limit): 1, 0.7, 0.3; 2, 0.5, 0.1; 3, 0.8, 0.7. Each expert generates output: +1 – in case the logical condition related to upper limit is true; -1 in case the logical condition related to lower limit is true; 0 – in case the previous conditions are false. Final decision is based on summed output divided by number of experts which is compared against the expert-acceptance-threshold TE.

Presented models have been implemented and examined in prepared simulation environment.

5. Simulation Environment and Simulation Results

All described models have been implemented in NetLogo environment.

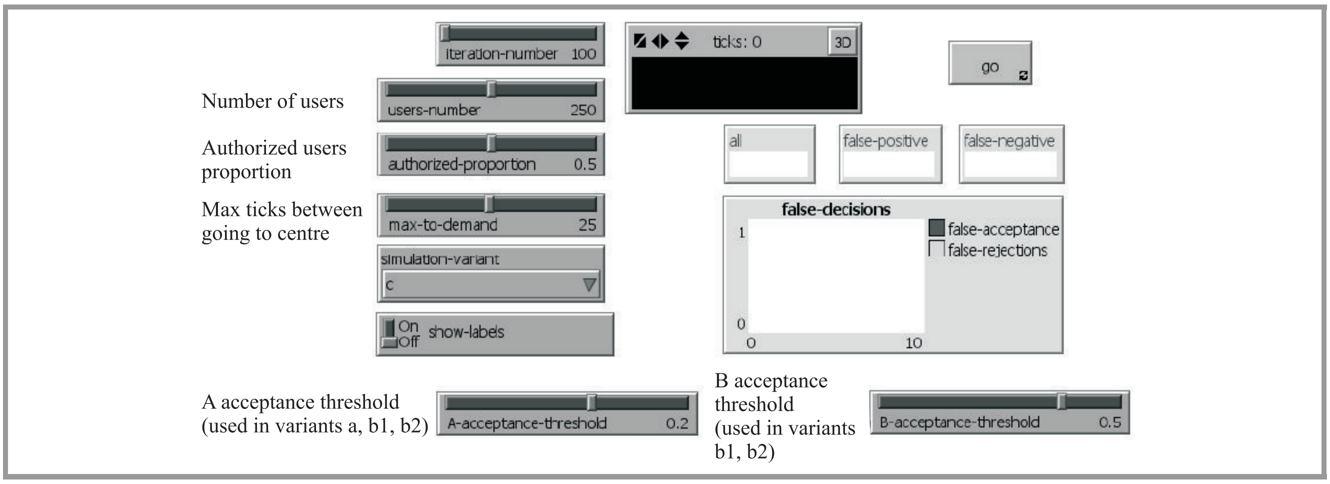
5.1. Simulation environment preparation

First, we have implemented:

- initialization procedures (setup-users, setup-centers, setup-experts),
- main procedures reflecting the four models (authenticate-a, authenticate-b1, authenticate-b2, authenticate-c),
- supporting procedures (setup, go, do-plots, etc.).

Next we have prepared the interface which consists of the following input controls:

- setup – which resets the values of environment controls to defaults,
- go – which starts the simulation,



iteration-number 100

users-number 250

authorized-proportion 0.5

max-to-demand 25

simulation-variant c

show-labels On Off

A-acceptance-threshold 0.2

B-acceptance-threshold 0.5

ticks: 0

Number of users
Authorized users proportion
Max ticks between going to centre
A acceptance threshold (used in variants a, b1, b2)
B acceptance threshold (used in variants b1, b2)
3D
go
all
false-positive
false-negative
false-decisions
1
0
0
10
false-acceptance
false-rejections

Fig. 3. Simulation environment.

- iteration number – which enables definition of length of simulation (expressed in ticks),
- users number – which enables definition of size of whole population,
- authorized proportion – which enables definition of structure of whole population,
- max-to-demand – which enables definition of the maximum number of ticks between going to authentication center,
- simulation variant – which enables choice of one of four implemented simulation models: a, b1, b2 and c,
- show labels – which enables switching on or off labels of the agents,
- auth-A-mean – which enables definition of average value of matching scores for genuine users using modality A),
- auth-A-stdev- which enables definition of standard deviation of matching scores of genuine users using modality A),
- auth-B-mean – which enables definition of average value of matching scores of genuine users using modality B),
- auth-B-stdev – which enables definition of standard deviation of matching scores of genuine users using modality B),
- auth-C-mean – which enables definition of average value of matching scores of genuine users using modality C),
- auth-C-stdev – which enables definition of standard deviation of matching scores of genuine users using modality C),
- unauth-A-mean – which enables definition of average value of matching scores of impostors using modality A),
- unauth-A-stdev – which enables definition of standard deviation of matching scores of impostors using modality A),
- unauth-B-mean – which enables definition of average value of matching scores of impostors using modality B),
- unauth-B-stdev – which enables definition of standard deviation of matching scores of impostors using modality B),
- unauth-C-mean – which enables definition of average value of matching scores of impostors using modality C),
- unauth-C-stdev – which enables definition of standard deviation of matching scores of impostors using modality C),
- A-acceptance-threshold – which enables definition of threshold for modality A,
- B-acceptance-threshold – which enables definition of threshold for modality B,
- C-acceptance-threshold – which enables definition of threshold for modality C.
- Experts-acceptance-threshold - which enables definition of threshold for preparing the final decision on the basing of votes of the experts.

Moreover we provide the output controls:

- World – which displays the simulation in 2D or 3D,
- Plot – which displays the false acceptance rate and false rejection rate,
- Reporter 1 – which displays number of performed authentications,
- Reporter 2 – which displays number of false acceptance decisions,
- Reporter 3 – which displays number of false rejection decisions.

The simulation environment window which combines enumerated controls is presented in Fig. 3.

5.2. Simulation Results

Each implemented model was executed being previously prepared according to specified values of given controls. During simulations the changes occurring in the environment were easily to be observed and they were logged in a comma seperated values file. Obtained values were used to prepare visualizations.
Here we present the initial values of given controls:

- iteration number = 100,
- users number = 250,
- authorized proportion = 0.5,
- max-to-demand = 25,
- show labels = off,
- auth-A-mean = 1.0,
- auth-A-stdev = 0.5,
- auth-B-mean = 1.0,
- auth-B-stdev = 0.5,
- auth-C-mean = 1.0,
- auth-C-stdev = 0.5,
- unauth-A-mean = –1.0,
- unauth-A-stdev = 0.5,
- unauth-B-mean = –1.0,
- unauth-B-stdev = 0.5,
- unauth-C-mean = –1.0,
- unauth-C-stdev = 0.5.

We conducted four group of simulations:

- First set of simulations were based on simulation model a. We were observing the false acceptance indicator (FA) and false rejection indicator (FR) in three different configurations of threshold TA (TA = 0.3, TA = 0.5 and TA = 0.7).
- Second set of simulations were based on simulation model b1. Again, se were observing the false acceptance indicator (FA) and false rejection indicator (FR) in three different configurations of threshold TA (TA = 0.3, TA = 0.5 and TA = 0.7) and threshold TB (TB = 0.3, TB = 0.5 and TB = 0.7).
- Third set of simulations were based on simulation model b2. Again, se were observing the false acceptance indicator (FA) and false rejection indicator (FR) in three different configurations of threshold TA (TA = 0.3, TA = 0.5 and TA = 0.7) and threshold TB (TB = 0.3, TB = 0.5 and TB = 0.7).
- Fourth set of simulations were based on simulation model c. We were observing the false acceptance indicator (FA) and false rejection indicator (FR) in three different configurations of experts-acceptance-threshold TE (TE = 0.3, TE = 0.5 and TE = 0.7).

In Fig. 4 we present how the FA and FR indicators were changing in simulated environment exploiting model a, for different (discrete) values of threshold TA.

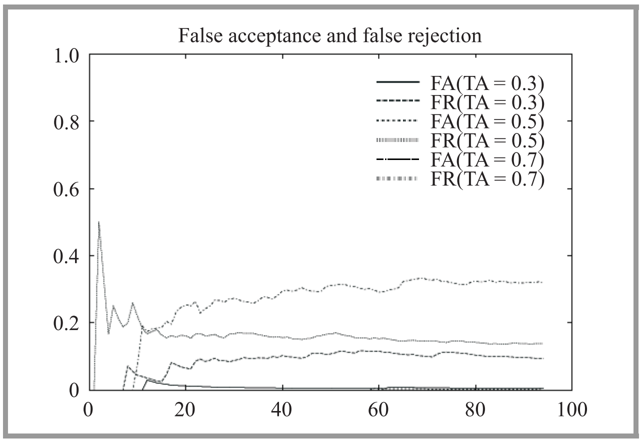


Fig. 4. Simulation results using model a.

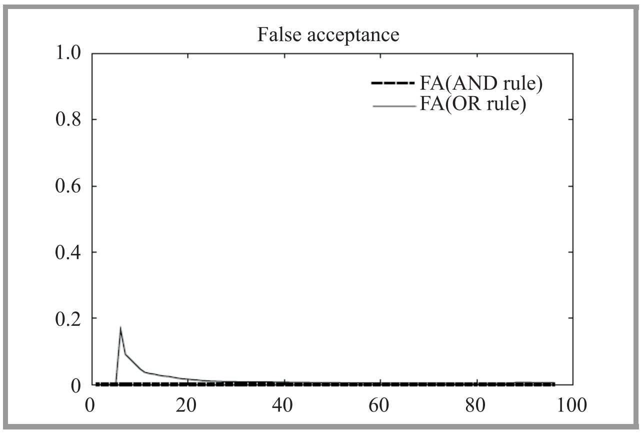


Fig. 5. Simulation results using models: b1 and b2 (FA indicator).

In Fig. 5 we compare FA indicators in simulated environment using models: b1 (AND rule) and b2 (OR rule). We use arbitrary set thresholds:

- TA = 0.3,
- TB = 0.5.

In Fig. 6 we compare the FR indicators in simulated environment using models: b1 (AND rule) and b2 (OR rule). Analogically, we use arbitrary set thresholds presented above.

The last simulation was performed using model c with three arbitrary set experts acceptance thresholds:

- TE = 0.3,
- TE = 0.5,
- TE = 0.7.

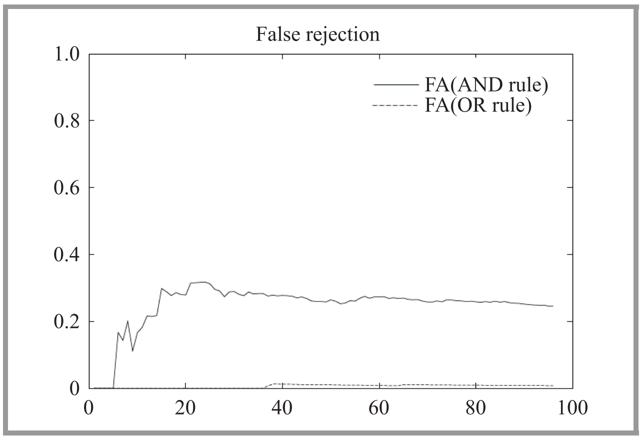


Fig. 6. Simulation results using models: b1 and b2 (FR indicator).

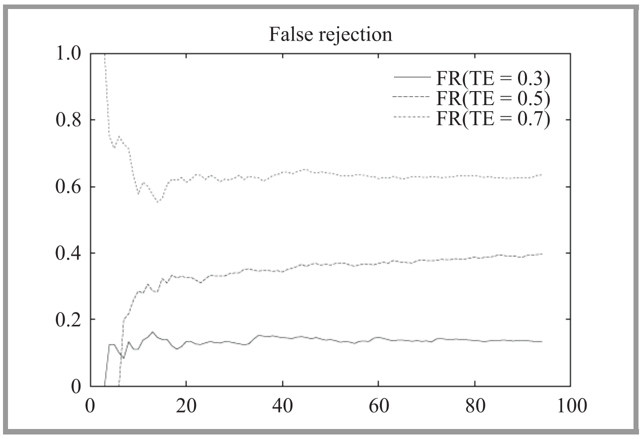


Fig. 7. Simulation results using model c (FR indicator).

The results of last simulation are presented in Fig. 7.

6. Conclusions and Further Work

In this paper authors applied multiagent paradigm in order to model single modal and multimodal biometric authentication systems. Four models were implemented using programmable modeling environment for simulating natural and social phenomena. Those models were appropriately parametrized and explored under various conditions. The implemented models enabled observing living environment with agents playing different roles (authenticator, authenticatee and other). The key benefit of proposed approach is the ability of observe how setting different input parameters influences the whole interactive system, as well as watch key performance indicators, i.e., false acceptance rate and false rejection rate. The results of undertaken (preliminary) research task are promising and convinced authors to formulate further research challenges. One of them is an introduction of several (instead of one) authentication centers and represent them in parallel or serial architecture. The second is related to development of learning authentication center exploiting individual instead of global thresholds. The third challenge will be associated with provision of detail parameters of selected biometric method as well as real biometric data.

References

[1] S. Sanchez and T. Lucas, "Exploring the world of agent-based simulations: simple models, complex analyses", in *Proc. 2002 Winter Simulation Conf.*, San Diego, USA, 2002, pp. 116–126.

[2] H. V. D. Parunak, "Practical and industrial applications of agent-based systems", Environmental Research Institute of Michigan, 1998.

[3] M. Wooldridge and N. R. Jennings, "Intelligent agents: theory and practice", *The Knowl. Engin. Rev.*, vol. 10, no. 2, pp. 115–152, 1995.

[4] S. Franklin and A. Graesser, "Is it an agent or just a program?: a taxonomy for autonomous agents", *Intelligent Agents III*. Berlin: Springer, 1997, pp. 21–36.

[5] S. Russell and P. Norvig, *Artificial Intelligence: Modern Approach*. Prentice Hall, 2002.

[6] M. Wooldridge, *An Introduction to MultiAgent Systems*. Chichester: Wiley, 2002.

[7] C. Macal and M. North, "Tutorial on agent-based modeling and simulation. Part 2: How to model with agents", in *Proc. Winter Simul. Conf. WSC 2006*, Monterey, USA, 2006, pp. 73–83, 2006.

[8] A. Rao and M. Georgeff, "BDI agents: from theory to practice", in *Proc. First Int. Conf. Multi-Agent Sys.*, San Francisco, USA, 1995, MIT Press, pp. 312–319.

[9] K. P. Sycara, "Multiagent Systems", *AI Mag.*, vol. 19, no. 2, Intelligent Agents Summer, pp. 79–93, 1998.

[10] C. Macal and M. North, *Managing Business Complexity. Discovering Strategic Solutions with Agent-Based Modeling and Simulation*. New York: Oxford University Press, 2007.

[11] M. Abreu and M. Fairhurst, "Analyzing the benefits of a novel multi-agent approach in a multimodal biometrics identification task", *IEEE Sys. J.*, vol. 3, no. 4, pp. 410–417, 2009.

[12] R. Meshulam, S. Reches, A. Yarden, and S. Kraus, "MLBPR: MAS for large-scale biometric pattern recognition", *Lect. Notes Comp. Sci.* (including Lec. Notes Artif. Int., Lec. Notes Bioinf.), pp. 274–292, 2009.

[13] G. Ali, N. A. Shaikh, and Z. A. Shaikh, "Towards an automated multiagent system to monitor user activities against insider threat", *in Proc. IEEE – Int. Symp. Biometr. Secur. Technol. ISBAST'08*, Islamabad, Pakistan, 2008.

[14] G. Chetty and D. Sharma, "Distributed face recognition: A multiagent approach", Lect. Notes. Comp. Sci. (including Lect. Notes Artif. Int., Lect. Notes Bioinf.), pp. 1168–1175, 2006.

[15] A. Canuto, M. Abreu, A. Medeiros, F. Souza, M. F. Gomes, and V. Bezerra, "Investigating the use of an agent-based multi-classifier system for classification tasks", in *Proc. 11th Int. Conf. Neural Inform. Proces. ICONIP'04*, Calcuta, India, *Lect. Notes Comp. Sci.*, Heidelberg: Springer, 2004, pp. 854–859.

[16] L. Huette, A. Nosary, and T. Paquet, "A multiple agent architecture for handwritten text recognition", *Patt. Recogn.*, vol. 37, no. 4, pp. 665–674, 2004.

[17] U. Wilensky, *NetLogo*. Center for Connected Learning and Computer-Based Modeling, Northwestern University, Evanston, IL, 1999 [Online]. Available: http://ccl.northwestern.edu/netlogo/

Tomasz Owczarek received the M.Sc. in management from the Silesian University of Technology in 2005, and the M.Sc. in mathematics from the University of Silesia in 2006. Currently he is a Ph.D. student in the Institute of Economics and Informatics at the Silesian University of Technology. His research interests are game theory, probabilistic graphical models and agent-based modeling and simulation.

e-mail: tomasz.owczarek@polsl.pl
Institute of Economics and Informatics
Silesian University of Technology
Roosevelta st 26-28
41-800 Zabrze, Poland

Adrian Kapczyński received the Ph.D. degree in computer science with honors from Silesian University of Technology in 2004. He is experienced in developing and customizing biometric solutions and Well-versed in areas such as database and network designing and administration. A member of IEEE, PIPS, ISACA, ACM and Mensa Polska.

e-mail: adriank@polsl.pl
Institute of Economics and Informatics
Silesian University of Technology
Roosevelta st 26-28
41-800 Zabrze, Poland