Acesso Inteligente: Uma porta capaz de aprender

Natalia C. de Amorim[1], Luis D. de N. Martins, Rogério R. de Vargas[1], and Cristiano Galafassi[1]

Laboratório de Sistemas Inteligentes e Modelagem (LabSIM), Federal University of Pampa, Itaqui-RS/Brazil
www.labsim.unipampa.edu.br

Abstract. Technology has provided efficiency and practicity for daily routines of people and companies. The market has solutions to flexibilize access that usually uses hard security controls that need cosntant actions from a manager. This way, the paper aims to formalize a control access model that uses artificial intelligence techniques to adapt the users behavior changes and presents a case study of the implementation of this model. It was verified that the model presented satisfactory performance and it is suggested, as future works, the use of neural networks to make a comparison with this work.

Keywords: agrupamento, ckMeansImage, fuzzy, sensoriamento remoto

1 Introdução

A expressão usual para demonstração de falta de inteligência "burro que nem uma porta" neste trabalho é questionada, nós mostramos que uma porta é inteligente e principalmente, é capaz de aprender.

A constante evolução da tecnologia traz consigo o aumento da demanda por inovações que tornem o cotidiano das pessoas e das empresas mais práticos. A "Internet das Coisas" (do inglês, *Internet of Things*) é uma mudança de tecnologia que conecta os dispositivos mais corriqueiras, isto é, do dia a dia à computação em nuvem. Cada vez mais surgem eletrodomésticos, meios de transporte e até mesmo tênis, roupas e maçanetas conectadas à internet e a outros dispositivos, como computadores e smartphones.

Atualmente existem no mercado inúmeras soluções afim de flexibilizar o acesso, basicamente todas utilizam um controle rígido de segurança onde um administrador libera, cadastra, altera ou exclui um usuário da entrada a um determinado recinto. Alguns sistemas utilizam de alguns mecanismos de multimídia para manipulação de conteúdo, que aplicadas são capazes de processar e transmitir alguns dados de mídia. Imagens, áudios ou textos são alguns exemplos. A Grande Enciclopédia Larousse Cultural[1] define multimídia como uma forma de comunicação com utilização de múltiplos meios como sons, imagens, textos, vídeos ou animações.

Esses sistemas, geralmente utilizam formas de acesso tradicionais, baseados em cartões magnéticos ou senhas para identificar os usuários, podendo ser

facilmente esquecido ou roubado. Um dos métodos mais utilizados é o sistema que utiliza identificação por rádio frequência RFID (Radio Frequency Identification), onde segundo [2], é uma tecnologia que utiliza ondas de radiofrequência para transmissão de dados. Esse sistema foi responsável pelo fortalecimento da Internet das Coisas, termo apresentado por [3], afirmando que a Internet das Coisas se define pela conexão de todos os objetos físicos à internet, com uma capacidade de obter informações por meio de identificação por radiofrequência e tecnologias de sensoriamento.

Instigado pela busca de maior confiabilidade nos sistemas de segurança, [4] construiu um controle de acesso utilizando Arduino, banco de dados MySql e LabView, onde utilizou a placa Arduino para programar e manipular o módulo RFID e o software LabView para unir todo esse conjunto e também desenvolver uma interface amigável ao usuário. Como meios alternativos e com baixos custos, plataformas abertas como o Arduino surgem para inovar e facilitar a construção desses projetos, possuindo diversos tipos de sensores como o próprio leitor RFID e vários outros, que auxiliam na execução do projeto. Segundo a própria empresa criadora, Arduino [5] é uma plataforma eletrônica de código aberto baseada em hardware e software fáceis de usar.

Além de aplicações comerciais, estudos científicos são realizados na área, buscando a criação de um sistema inteligente para controlar e gerir o acesso. Nesse contexto, [6] apresentam um sistema de autenticação inteligente baseado em um sensor biométrico que apresenta muitas vantagens, como pequeno volume, baixo consumi energético, baixo custo, segurança e confiança, entre outros. Posteriormente, [7] complementam o trabalho acoplando um sistema de alarme wireless com o objetivo de conseguir um sistema de controle simples e que responda em tempo real.

Em [8] apresenta-se um modelo de sistema automatizado de autenticação de acesso de estudantes baseado em impressão digital. O modelo consiste em um sistema de captura a impressão digital, processamento de informações e liberações de acesso mediante cadastro prévio. As informações referentes ao acesso são registradas e armazenadas em um servidor que disponibiliza as informações online. Os autores argumentam que esse sistema reduz a carga de trabalho dos responsáveis em manter o registro dos acessos realizados.

Em [8] propõem-se uma abordagem mais robusta utilizando Arduino, onde as informações passam a ser registradas em um servidor, de modo a facilitar o trabalho manual dos gestores. Contudo, em ambos os trabalhos, o cadastro biométrico deve ser realizado em cada unidade de acesso (*i.e.*, em cada porta), o que inviabiliza a utilização em larga escala (*i.e.*, em uma universidade).

Estimulados por uma necessidade de controle e gestão de laboratórios, buscou-se técnicas que pudessem servir de aporte para sustentar um modelo inteligente de controle e gestão de acesso. Nesse contexto, a Inteligência Artificial (IA) surge para fomentar a proposta. Em [9] define-se IA como a ciência e engenharia de produzir máquinas inteligentes. Em [10] apresenta-se uma definição similar, onde apontam que computação inteligente é o estudo do desenvolvimento de agentes inteligentes, onde um agente pode ser definido como

uma entidade autônoma que percebe seu ambiente, se adapta às mudanças e persegue seus objetivos.

Inspirando-se nesses conceitos e nos trabalhos citados, essa proposta tem o objetivo de definir formalmente um modelo de sistema de controle e gestão de acesso que aprenda e se adapte as mudanças de comportamento dos usuários através de técnicas de inteligência artificial. O presente trabalho diferencia-se dos demais pela capacidade de ser ampliado para inúmeras unidades de acesso, possuindo um cadastro único centralizado e perfis de acesso descentralizados. Para tal, utiliza-se uma arquitetura multiagente que permite o controle, validação de acesso, aprendizado e adaptação aos usuários.

O trabalho está organizado no que segue. Na Seção 2 são apresentados conceitos de Aprendizado Supervisionado, Sistemas Multiagentes, e Lógica Fuzzy. A seguir, na Seção 3 formaliza-se o modelo proposto de acesso inteligente e um estudo de caso é apresentado na Seção 4. Ao final, na Seção 5, são apresentadas as conclusões.

2 Estado da Arte

As técnicas de inteligência artificial utilizadas neste trabalho são transcritas de forma sucinta nas próximas subseções.

2.1 Apredizado supervisionado

Aprendizagem supervisionada é uma tarefa de aprendizagem de máquina que tem como objetivo inferir uma função a partir de dados de treinamento rotulados [11]. Os dados de treinamento consistem de um conjunto de exemplos de treinamento. Na aprendizagem supervisionada, cada exemplo é um par constituído por um objeto de entrada (tipicamente um vetor) e um valor de saída desejado (também chamado o sinal de controle). Um algoritmo de aprendizagem supervisionada, analisa os dados de treino e produz uma função de inferência, que pode ser utilizada para o mapeamento de novos exemplos.

De modo geral, a aprendizagem supervisionada é adequada para qualquer problema em que deduzir uma classificação seja útil e que a classificação seja fácil de determinar. Além disso, conforme aponta [12], o software pode ter um conhecimento a prior, definido pelas características do problema, e tenha que se adaptar, aprendendo com um crítico externo. Desse modo, o software necessita converter a informação do crítico em um rótulo para a entrada recebida, ou em um valor de recompensa, caso o software tenha classificado antes da resposta do crítico.

2.2 Sistemas Multiagentes

Um sistema multiagente (SMA) é um sistema computacional em que dois ou mais agentes interagem ou trabalham em conjunto de forma a desempenhar determinadas tarefas ou satisfazer um conjunto de objetivos [13]. Segundo [14],

um agente é um sistema computacional encapsulado que está situado em um ambiente e que é capaz de ser flexível e agir autonomamente para atingir seus próprios objetivos.

De acordo com [15], os agentes geralmente possuem uma esfera de visibilidade e influência limitada pelas suas funções e seus objetivos. Desse modo, cada agente interage com um número limitado de outros agentes, definido explicitamente pela arquitetura do modelo ou emergindo do comportamento de cada agente ao buscarem seus objetivos. Em um SMA, os agentes podem ser homogêneos ou heterogêneos e apresentam três características:

- Decomposição: permite abordar cada subproblema de maneira independente, permitindo a abordagem de um problema por vez, reduzindo a complexidade;
- Abstração: permite definir um modelo simplificado do problema, dando ênfase aos aspectos pertinentes e ocultando detalhes irrelevantes;
- Flexibilidade: sistemas complexos necessitam de componentes de comportamento autônomo e flexível, pois componentes de software precisam interagir.

2.3 Lógica Fuzzy

A lógica *fuzzy* proposta por [16] concebida como um resultado de uma tentativa de lidar com a imprecisão.

Na teoria Clássica de Conjuntos, um elemento pertence ou não pertence a um determinado conjunto. Atribuindo um grau pertinência, um valor compreendido entre o intervalo zero e um, a restrição de pertencer ou não pertencer a um conjunto é enfraquecida. Na teoria dos conjuntos (clássica) um conjunto admite uma forma alternativa de ser representado via uma função que mapeia um elemento do universo ao valor 1, se esse elemento fizer parte do conjunto e zero caso contrário. Formalmente, dado um conjunto A no universo U, a função $\chi_A : U \to \{0, 1\}$ definida na Equação (1), é chamada de função característica de A.

$$\chi_A(x) = \begin{cases} 1, \text{ se } x \text{ é um elemento do conjunto } A, \text{ e} \\ 0, \text{ se } x \text{ não é um elemento do conjunto } A \end{cases} \tag{1}$$

Na teoria dos conjuntos *fuzzy* um elemento pode pertencer parcialmente a um dado conjunto. O grau de pertinência é definido através de uma generalização da função característica chamada de *função de pertinência* e é definida pela Equação (2).

$$\mu_A(x) : U \to [0; 1] \tag{2}$$

onde U chama-se conjunto universo e A é conjunto fuzzy.

Os valores da função de pertinência aplicada a elementos do universo de discurso são números reais no intervalo $[0; 1]$, onde 0 significa que certamente o elemento não é membro do conjunto e 1 significa que o mesmo pertence absolutamente ao conjunto. Cada valor da função de pertinência é chamado de *grau de pertinência*.

Entre diversas operações entre conjuntos fuzzy, citamos a união e intersecção, que são usadas neste artigo. A união e a intersecção de dois conjuntos *fuzzy* A e B do universo U é definida de diversas formas na literatura. Por exemplo, pode-se representar $A \cup B$ pela função de pertinência como mostrado na Equação (3).

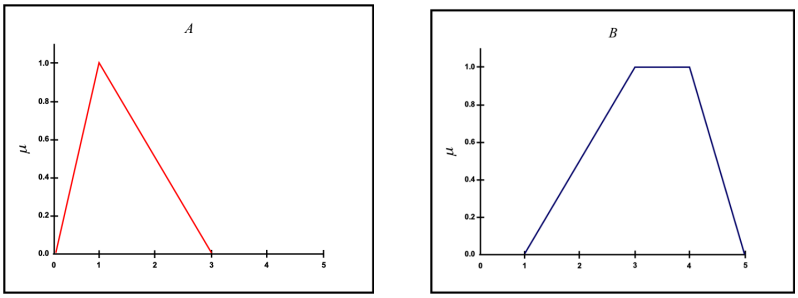
$$\mu_{A \cup B} = max[\mu_A(x_i); \mu_A(x_i)] \tag{3}$$

Já a intersecção entre dois conjuntos $(A \cap B)$ pode-se representar conforme a Equação (4).

$$\mu_{A \cap B} = min[\mu_A(x_i); \mu_A(x_i)] \tag{4}$$

A Figura 1 mostra o conjunto A (Figura 1(a)), o conjunto B (Figura 1(b)) e a plotagem entre os conjuntos A e B na Figura 1.

Exemplo de dois conjuntos fuzzy A e B.



(a) Conjunto A (b) Conjunto B

Fig. 1. Conjuntos A e B

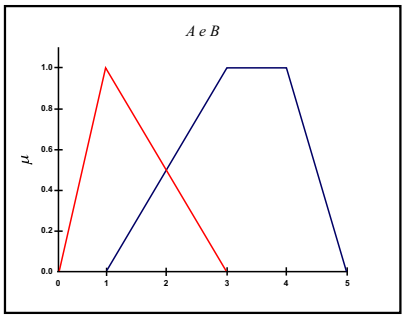


Fig. 2. Conjunto A e B

3 Proposta de Acesso Inteligente

Definimos acesso inteligente como um sistema que seja capaz de aprender, quando for realizada uma liberação de acesso fora do tempo pré-programado e, consequentemente, sugerir um novo perfil de acesso, minimizando o trabalho do administrador.

Por se tratar de um sistema multiagente, trabalha-se com a ideia de ambiente distribuído, onde cada agente possui objetivos distintos e busca atingir suas metas. Por outro lado, a informação referente ao perfil de acesso é gerida de forma centralizada, de modo a evitar a perda ou alteração indevida do perfil de acesso.

O processo pode ser realizado de duas formas distintas. A primeira se inicia através de uma solicitação de acesso por parte do usuário, por meio de uma identificação única. O agente *Door* envia o código biométrico obtido do usuário através de um *webservice* para o agente *Profile* que, por sua vez, se comunica com o agente *Expert*, informando que determinando usuário tentou realizar um acesso em local específico. Com base nas regras de acesso já estabelecidas, o agente *Expert* responde ao agente *Profile*, informando se o acesso deve ser permitido. O agente *Profile* armazena um histórico de acesso, sendo ele permitido ou não, e envia uma mensagem ao agente *Door*, para que o mesmo libere o acesso ou informe ao usuário.

O segundo processo é realizado de forma indireta, onde o usuário solicita ao administrador que o acesso seja liberado. Nesse momento, o administrador poderá realizar a liberação de acesso através de um dispositivo (*i.e.*, computador, celular, *tablet*). Essa informação é encaminhada para o agente *Profile*, o qual registra o histórico de acesso e solicita que o agente *Door* libere o acesso. Sempre que for informada a identificação do usuário que deseja acessar o determinado local, o agente *Profile* encaminha uma mensagem ao agente *Expert*. Desse modo, o agente *Expert* tem a possibilidade de incorporar essa informação as suas regras de acesso. Nesse momento, o agente *Expert* poderá aprender uma nova regra de acesso e sugerir ao administrador que a mesma seja incorporada no cadastro do usuário, diminuindo o trabalho do administrador em tentativas de ingresso futuras.

Para ilustrar a proposta, a Figura 3 mostra detalhadamente os componentes que compõem o modelo.

A definição de cada componente é mostrada a seguir:

1. *Agent Door (Agente porta)*: Este agente identifica o usuário, comunica o responsável e libera o acesso;
2. *Webservice (servidor de serviços web) / FIPA:* Provedor de serviços web para realizar a comunicação entre os agentes utilizando padrão de comunicação FIPA (Foundation for Intelligent Physical Agents);
3. *Agent Profile (Agente perfil):* Este agente tem a função de monitorar e guardar o histórico de acesso e liberação dos usuários por parte dos administradores;
4. *History (histórico):* Registros do sistema;

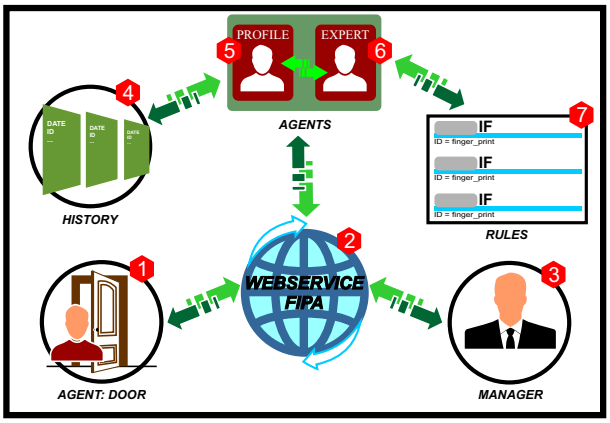


Fig. 3. Esquema de acesso inteligente.

5. *Agent Expert (Agente Especialista):* O agente especialista aprende as regras de acesso a serem sugeridas para o administrador e consulta suas regras para decidir se o acesso pode ser permitido;
6. *Rules (Regras):* São as regras de acesso;
7. *Manager (Administrador/Responsável):* É o responsável pelo acesso, é o administrador do local.

3.1 Aprendizado de regras de acesso

A cada acesso i para o local d liberado pelo administrador o algoritmo de aprendizado é executado, cuja a entrada é composta por um vetor (κ, α, μ), onde κ define quantas entradas iniciais são necessárias para o sistema iniciar o aprendizado, α que é o grau mínimo de pertinência em μ e μ é o grau de pertinência.

A definição formal é dada pela Equação (5).

$$Ars_d = \begin{cases} Ap_d \cup Al_{di}, \text{ se } \gamma_{di} \geq \alpha \\ Ap_d, \text{ caso contrário} \end{cases} \tag{5}$$

onde:

- Ars_d é o acesso resultante sugerido para o local d;
- Ap_d é o acesso programado pelo responsável para o local d;
- Al_{di} é o acesso liberado para o local d no momento i;
- $\gamma_{di} = \max \mu_{Ap_d \cap Al_{di}}$.

4 Estudo de Caso: Acesso a um laboratório

Seguindo as definições citadas na seção anterior, aplicou-se o modelo de controle e gestão de acesso inteligente a um laboratório de pesquisa em uma universidade.

Para gerenciar o acesso local a este laboratório (Agente *Door*), as especificações de hardware são: uma placa de prototipagem (arduíno uno), uma fechadura eletrônica (fecho eletrônico) e um leitor de impressão digital.

Em um servidor web foram criados os agentes *Profile* e *Expert*, além do histórico e das regras de acesso. Essas informações são armazenadas em um banco de dados cujo o modelo entidade relacionamento (Modelo ER) é mostrado na Figura 4.

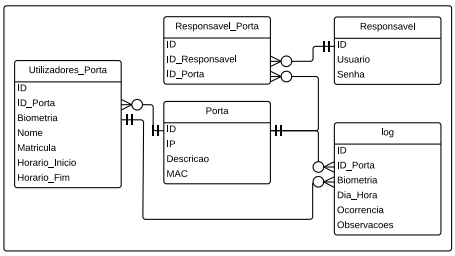


Fig. 4. Modelo ER do estudo de caso.

A entidade *Utilizadores_Porta* consiste nos usuários do laboratório, a entidade *Porta* define o cadastro do local de acesso, a entidade *Responsável* define o cadastro do administrador do laboratório, a entidade *Responsavel_Porta* relaciona os administradores ao laboratório e a entidade *log* compõem o histórico. Ainda assim, as regras são definidas na entidade *Utilizadores_Porta* e o agente *Manager* é indiretamente modelado pelo *Administrador*.

Os parâmetros definidos a priori são: $\tau = 20$ minutos, $\alpha = 0,5$ para o corte e $\kappa = 2$ ocorrências.

As Figuras 5, 6(a) e 6(b) ilustram um estudo de caso onde o usuário X teve seu acesso cadastrado entre 7:30 às 9:20 (Figura 5) pelo responsável do laboratório.

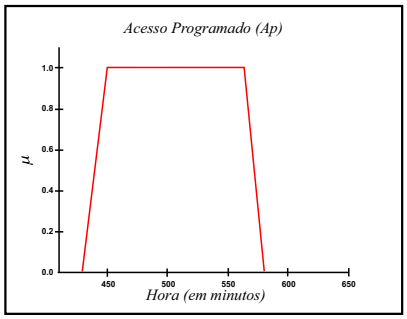
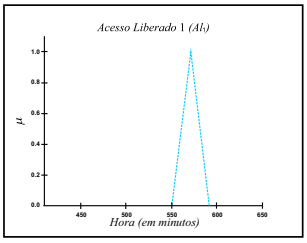
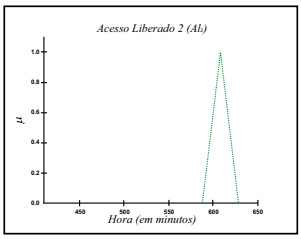


Fig. 5. Acesso das 7:30 às 9:20.

Em outro momento X solicitou a entrada fora do horário cadastrado, sua solicitação deu-se no horário 9:31 (Figura 6(a)) e às 10:11 (Figura 6(b)), ambas solicitações foram deferidas pelo responsável do laboratório.



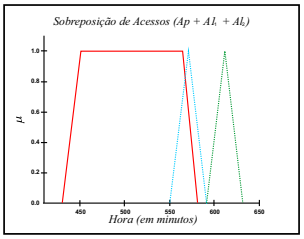
(a) Acesso liberado às 9:31



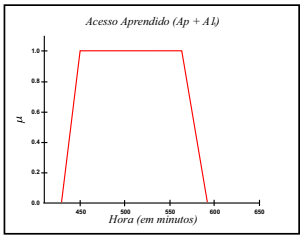
(b) Acesso liberado às 10:11

Fig. 6. Solicitações deferidas pelo responsável

Diante destas liberações, um perfil de novo acesso do usuário X é criado. As Figuras 7(a) e 7(b) mostram que o sistema inteligente aprende e sugere ao responsável que o usuário X possa ter acesso. A Figura 7(a) mostra os três acessos permitidos e a Figura 7(b) mostra o horário sugerido pelo sistema inteligente, respectivamente.



(a) Sobreposição de acessos



(b) Acesso aprendido das 7:30 às 9:41 com $\alpha = 5$

Fig. 7. Acessos e aprendizado ocorrido

Conforme pode ser visto, as Figuras 7(a) e 7(b) mostram o acesso aprendido das 7:10 e 9:41 considerando apenas o acesso Al_1. Uma vez que $Ap \cap Al_2$ possui $\alpha = 0$, desconsiderou-se o registro.

Desse modo, caso seja aceito pelo responsável os novos horários em que o usuário pode ter acesso fica entre 7:10 e 9:41 conforme definido pelo α de 0,5.

5 Conclusões

A "Internet das coisas" é um conceito tecnológico em que todos os objetos da vida cotidiana estariam conectados à internet, agindo de modo inteligente e sensorial. Faz com sucesso a transição de um conceito futurista à realidade tangível. Do ponto de vista da indústria de software, a avaliação também é de que esta tecnologia está em plena aceleração.

Com o crescimento da economia e sociedade, as pessoas exigem segurança, praticidade e precisão na tecnologia de autenticação, isto é, ao acesso a um determinado local. Um sistema de controle e gestão de acesso inteligente, pode ser definido de forma sucinta como: "aprender e se adaptar no decorrer dos acessos". Apresentou-se a modelagem formal da proposta e um estudo de caso onde sugere-se um modelo baseado em entidades e relacionamentos para armazenar e gerenciar as informações. Ainda no estudo de caso, mostramos uma situação em que o sistema inteligente aprende uma nova configuração de perfil de acesso. Como trabalhos futuros, pretendemos criar outras técnicas de aprendizado de acordo com o perfil de acesso do usuário, utilizando técnicas de redes neurais, e comparar com a proposta *fuzzy* apresentada neste trabalho.

References

1. Ducrocq, A.: Grande EnciclopÃ©dia Larousse Cultural. Larousse, SÃ£o Paulo (1998)
2. Barbosa, R.P.: RFID - Radio Frequency identification. (2012) Instituto de MatemÃ¡tica e EstatÃstica da USP. Monografia desenvolvida para a disciplina de ComputaÃ§Ã£o MÃ³*veldoProgramadeP*^{3}*s* − *gradua*§*£oemCi*^{a}*nciadaComputa*§*£o*, *S£oPaulo*, *Brazil*.
3. Ashton, K.: That 'Internet of Things' Thing. RFID Journal (2009)
4. Custodio, R.A.: Controle de Acesso utilizando Arduino, Banco de dados MySql e Labview. (2015) Universidade Estadual Paulista. Faculdade de Engenharia de GuaratinguetÃ¡. GuaratinguetÃ¡, Brazil.
5. Arduino: What is arduino? (2017)
6. Wang, F., Zhang, Y.: Study and design of intelligent authentication system based on fingerprint identification. In: Proceedings of the 2009 Second International Symposium on Knowledge Acquisition and Modeling - Volume 03. KAM '09, Washington, DC, USA, IEEE Computer Society (2009) 170–173
7. Wang, Y., Liu, H., Feng, J.: The design of an intelligent security access control system based on fingerprint sensor fpc1011c. Circuits and Systems **1**(1) (2010) 30–33
8. Jalundhwala, A., Jhaveri, P., Khudanpur, S., Deshmukh, A.: Article: Wireless fingerprint attendance marking system. International Journal of Computer Applications **108**(8) (December 2014) 1–5 Full text available.

9. McCarthy, J., Minsky, M., Rochester, N., Shannon, C.E.: A proposal for the dartmouth summer research project on artificial intelligence, august 31, 1955. AI Magazine **27**(4) (2006) 12–14
10. Russell, S., Norvig, P.: Artificial Intelligence: A Modern Approach. 3rd edn. Prentice Hall Press, Upper Saddle River, NJ, USA (2009)
11. Mohri, M., Rostamizadeh, A., Talwalkar, A.: Foundations of Machine Learning. The MIT Press (2012)
12. Ballard, D.: An Introduction to Natural Computation. Bradford Books. MIT Press (1997)
13. Wooldridge, M.: An Introduction to MultiAgent Systems. 2nd edn. Wiley Publishing (2009)
14. Wooldridge, M.: Agent-based software engineering. IEE Proceedings-software **144**(1) (1997) 26–37
15. Jennings, N.R.: On agent-based software engineering. Artif. Intell. **117**(2) (March 2000) 277–296
16. Zadeh, L.: Fuzzy Sets. Inf. Control **8** (1965) 338–353