Journal of Engineering and Applied Sciences 13 (13): 4905-4912, 2018
ISSN: 1816-949X

DA Conceptual Security Sub-Model for Enhancing Human-Agent Collaboration Based on Generic Nodal Approach

[1]Khudhair Abbas Mohammed, [1, 2]Muamer N. Mohammed,
[1]Mazlina Abdul Majidmohd and [3]Mohd Sharifuddin Ahmad
[1]Faculty of Computer Systems and Software Engineering,
[2]IBM Center of Excellence, University Malaysia Pahang, 26300 Kuantan, Pahang, Malaysia
[3]College of Graduate Studies, University Tenaga Nasional, Kajang, Selangor, Malaysia

Abstract: Security aspects are serious issues for multi-agent systems that should be taken into consideration when designing the systems. The significant effects and outcomes of the software agent technology make its application more and more popular in several fields. The rapid development of the agent technology promotes its ability to be applied in many different areas such as transportation, e-Business and healthcare. However as with any other systems, the agent technology is also vulnerable to security threats and consequently, there is a need to equip the system's functionalities with some security defense system. A number of methodologies are providing methods and techniques for constructing security for multi-agent systems. A survey of the current state-of-the-art of security issues for MAS is the aim of this study. Techniques and models for securing multi-agent systems are presented in this study which is categorized according to the concepts and models regarding agent's and system's functionalities. Additionally, possible threats and attacks on multi-agent systems are defined and considered with agent's roles and communications concerns. Moreover, up to date security solutions are elaborated at both levels: agent and the system levels. Finally, an analysis of existing work problems and the challenges of future research for the security of multi-agents are presented.

Key words: Software agents, multi-agent system, security aspects, nodal approach, techniques, transportation

INTRODUCTION

The traditional methods techniques of developing software systems are no more applied, especially when the facilitations of agents are expanded arises. Gradually, facilitations of agents improved several devices to become more cognitive and intelligent within its environment. Such devices are developed with software agents that can autonomously decide and accomplish its aim to satisfy user's objectives. The software agent technology is a prevalent paradigm that is increasingly popular in its application within organizations. However, for an agent to achieve its intended goal, it should have the ability to communicate and interact with other parties which could be agents and/or humans.

Simply put agents are considered as a group of computational entities that can perform tasks on behalf of their owners (Ramchurn *et al*., 2016). An agent has the influence to collaborate with other agents to achieve its goal. Collaboration is one of the key aspects of agent's activities. It provides the necessary actions when an agent performs complex tasks. These collaborations use some mechanisms and actions to execute a secure performance such as message exchanges. Message exchanges are autonomously performed without human intervention to resolve problems with other agents in the same system. A typical agent architecture is designed with Beliefs, Desires and Intentions (BDI), processing instructions that enable the agent to autonomously perform actions in its lifecycle.

Collaboration systems allow workers to solve a problem that is beyond their capabilities or knowledge (Majid *et al*., 2016). Due to the distributed nature of heterogeneous systems, the objectives of a MAS are achieved when a variety of agents communicate and collaborate with each other (Mohammed *et al*., 2014). The interactions made with other agent creates a virtual society that fulfills the reason for its existence. Such virtual society allows the MAS to implement the complexities of real world issues. Some complex systems comprise of multiple agents which interact with each other to achieve some goals. Multi-agent systems provide designers with more flexibility by creating agents with many functions (Hanna and Richards, 2012).

Corresponding Author: Khudhair Abbas Mohammed, Faculty of Computer Systems and Software Engineering, University Malaysia Pahang, 26300 Kuantant, Pahang, Malaysia

Collaboration, communication and intelligence are the critical functions with which agents should be designed. Such agent functions support the design of complex systems and making it closer to a real-world human society (Majid, 2011).

Multi-agent systems are widely used in complex applications such as industrial, commercial, governmental, military, entertainment and healthcare applications. Each agent has special abilities to perform tasks and it is specialized with certain capabilities to assist humans in their daily work. An agent is beneficial to humans when the agent assists to reduce the task's complexity. In many circumstances interfaces are provided to handle communication and task's exchanges between humans and agents. Agents are currently applied in both small applications such as email filters and personal assistants as well as open and complex applications such as air traffic control, military demining, logistic planning, financial portfolio management, among others (Shih *et al*., 2013).

The particular capabilities of MAS are expanding when internet services are provided due to the availability of wide-area networks. Consequently, MAS including the autonomous systems, improve the choice for building complex and adaptive software applications agents in distributed MAS are usually interconnected and collaborate in utilizing the systems information and resources for goal achievement. Additionally, distributed MAS offer significant benefits to the system such as enhanced decision-making, suggest solutions and separating expertise.

However, in order to develop multi-agent systems that use the internet to interconnect the agents, security aspects should be implemented. MAS rely on collaboration between humans and agents which make it more vulnerable to interact with strangers. Systems in heterogeneous environments in which agents reside are open to security threats. A multi-agent system is similar to other systems when using the network, threaten by malicious actions and other security problems. The security problems in these environments which must not be neglected include malicious actions, blocking of resources, breach of information integrity and breach of private data. Additionally there are several vulnerabilities of MAS when connected to an open-network (Adameit *et al*., 2010). Malicious entities in the environment of open-network may cause problems by rendering agents to misbehave or vulnerable to attack. By exploiting an agent's social ability, these entities applied in heterogeneous systems could force the agent to misbehave and redirect its result to the hacker's destination.

One of the techniques that attackers use to deceive is to use a masquerade agent that acts similarly to a real agent in a certain environment and steal valuable data and perform malicious actions. Attackers can also persuade an agent to perform mischievous tasks by observing data that belongs to other agents. For example in financial systems in which MAS are used to support team decision-making such systems may be inheritably unsafe. Such systems demonstrate a failure resolve security problems when a huge amount of data or online banking transactions are wrongly transferred by attackers. Furthermore, numerous insecure actions may occur and put the organization in a serious danger. In order to avoid these security threats organizations (such as healthcare administration and e-business) that depend on MAS, must install and deploy security systems within the organization.

The main purpose of this study is to identify the use of security systems in MAS and summarize the literature in related works.

Literature review: Several attempts have been made to identify the vulnerabilities in the Multi-Agent Systems (MAS). Security in computing is a platform that provides solutions which can contribute to resolving these vulnerabilities. Consequently, it is critical and important to protect data from being tampered or hacked by malicious actions. The term computer security does not have a unique definition by researchers. Security in MAS is quite susceptible to threats compared with other systems that make use of centralized performance. Many components of MAS are decentralized and deployed in different areas. Hence, it essential to promote multi-agent systems deployed with security aspects.

Researchers have proposed a diversity of techniques and methods to ensure that multi-agent systems are secured from attackers. Yue *et al*. (2009) propose a security model to prevent a colluded truncation attack which focuses on a sent message and modifies it. This attack comprises of two malicious agents which connect to a sender agent and conspire to change its message. Another technique presented by Becker-Asano and Wachsmuth (2010) in which an inference system is provided. The assistance of inference system is to tell and estimate the users about a malignant part and can be detected by the whole system. Even though their system is not established for MAS, it can be used to keep MAS safe from malevolent parts. Backer provides his framework based on the secrecy of policy language analysis.

Clark *et al*. (2010) propose a framework for a particular Service Level Agreement (SLA) that involves methods to dynamically protect and maintain reliable violation

monitoring policies. Clark uses a web service for an SLA specification which he implements in agentscape. The reason for utilizing the web services is to test and establish an agreement among participants in a centralized and decentralized monitoring. Clark framework offers usefulness of results when it is applied in decentralized systems.

Nowadays, many devices that use networks to join and share data need smart utilization to safely prevail in several areas. Definitely, security perspective considers a smarter utilization due to software vulnerabilities that cause huge problems (e.g., e-Commerce field). Security applications continuously improve system's devices with data theft invasion detection, fire detection, personal health protection, etc. Nevertheless, there are deficiencies to fully secure network devices and equip them with flexibility to serve users. Therefore, several systems have been proposed to enhance and construct security services by providing monitoring sensors, controlling parameters and robots. Moradian (2013) in the study entitled "Security of e-Commerce software systems" suggest using intelligent agents to develop business processes. The researchers show in their study the facilitation, implementation and design of the agent technology to support engineers during the development process. The proposed system enacts various security services in an e-Commerce system which assist engineers to monitor decisions and activities; Search for security measures and mechanisms; Perform checks and provide advice and feedbacks.

MATERIALS AND METHODS

Security service provision for mas: Numerous multi-agent based systems are being developed with practical applications such as the multi-agent based marketplace (Macal and North, 2014). However, in such systems often the developers tend to overlook important security features. This only leads to loss of confidence in such systems. Standard mechanisms for specifying security in multi-agent systems must be developed.

Multi-agent systems with practical applications are developed in a variety of domains (Majid *et al*., 2009). Unfortunately, researchers often fail to include a security level in their systems, depending solely on the network security schemes. Security cannot be ignored due to its importance in developing systems. While basic security is important, gradually, confidentiality and authentication will be weaknesses to such systems. In order to solve this matter, the developer must design multi-agent systems with security in mind.

So far, there is no standard security model for MASs, although, various security models have been proposed in the literature. Poslad *et al*. (2002) propose the asset security model in which security is defined as a set of safeguards that help protect the assets. They define the communication service, the name service and the directory service as the core MAS assets and then describe threats and safeguards for each.

Mouratidis *et al*. (2003) propose security concepts which enable the tropos methodology to model security concerns throughout the entire MAS development process. Tropos (Bresciani *et al*., 2004) has been proposed as an agent-oriented software engineering methodology but it does not consider security.

Hence, Bresciani *et al*. (2004) add security to tropos methodology by employing various security concepts such as security constraint and security dependency, security entities such as secure goal and secure task and a security reference diagram. As an initial step, they introduce an algorithm that identifies and break security bottlenecks to reduce the complexity and criticality of MASs. They have extended Tropos to propose the secure Tropos Model (Mouratidis and Giorgini , 2007).

Potential threats and attacks: In the past decade, researchers have attempted to work on and develop agent-oriented software engineering methodologies. In fact, Gaia, one of these methodologies, provides various approaches in modeling multi-agent systems. But the development stages of such methodologies neglect the security aspects in design which few researchers seek to handle (Sawa *et al*., 2016). In a typical organization, systems that use MAS can be crippled by cybercriminals which could ruin the business operation of the organization. Accordingly, agent behavior at some stage of operation should evolve, so that, its patterns of strength and capabilities should reduce the system's risks. In cybercrimes, deception shapes an intricate information and costs an organization both financially and administratively. These ruin the organization's reputation and image which is the objective of those criminals. Eventually, the threats mentioned above motivate the needs for security that should be considered early in the development stage.

Human vulnerabilities incite attacker's to hack systems in organizations which are hard to protect. Numerous researchers have identified and improved significant issues regarding the development of security approaches and system design. Therefore, security approaches incorporate both the design and implementation part of system functionalities. Information assets are protected once security is established in the development of MAS. The information assets and security include confidentiality integrity and availability (Mouratidis and Giorgini, 2007). Building a secure MAS

increases the degree of information confidentiality integrity and availability. Sawa *et al.* (2016) introduce an approach using natural language processing techniques for two purposes: first is to detect a social engineering attack, Second is to identify suspicious comments fabricated by attackers.

The researchers focuses on social engineering attacks which is divided into private information and command requests. Sawa *et al.* (2016) approach applies questions to the listener by performing tasks. The speaker is not authorized to perform any of these tasks before it uses a technique to detect questions and commands and extract their likely topics and finally determine which one is malicious. This approach employs the benefits of text dialogues in order to evolve its applicability and functionality on many attack vectors. However, a prime limitation to this approach is applicability because the openness of such approach refuses many traditional security solutions.

Although, applicable approaches in MASs award them an attractive behavior for various new applications, new problems arise, among which security is a key. Most of these applications are used in the real world, the need for security increases. Consequently, researchers apply their approaches to analyze several attacks and provide users and system designers with obvious and high detection technique (Mohammed *et al*., 2014). Fortunately, there are several researchers who are working to address the potential gaps in the security of multi-agent systems and limit its vulnerability.

For example, Casey *et al.* (2016) focus on cyber security which relies on the private and asymmetric information which is significant to agent utilities. Furthermore, his approach provides an agent behavior decision when it links with an advanced model using signaling method. In addition, the nature attributes of MASs that utilizes an agent to perform its tasks in miserable systems where the traditional security techniques prevail, confer attacker to distort system data while new risks are appeared (Bijani and Robertson, 2014).

Security threats and risks enclose MASs and minimize its perfect performances and influence its outcomes. Consequently, these weaknesses need to study and detect to decrease the attacker's deception appetite. The vital features of multi-agent systems such as autonomy, openness and independence of multi-agent systems increase the value of being threatened, especially when connected to the human. Agents capabilities of interactions with humans and/or other agents enlarge the security difficulties in MASs which is an assumptive factor to keep the data of such systems safe. Phishing, spoofing, sybil, elicitation and webpage compromises (Hornok *et al*., 2014; Gonzalez *et al*., 2008) are some examples of vulnerabilities of MASs used by attackers via. social engineering for their diabolical scheme. Consequently, social engineering is considered as an important and significant subject that should be intensely analyzed by cyber security designers.

Threats and attacks in multi-agent systems are not fully studied and understood by researchers. Since, MASs are gradually implemented in many distributed systems, it is imperative that designing such systems should entail a comprehensive and detailed analysis of security requirements. For instance, system's information is considered as prime risks due to insider threats and attacks. Subsequently, security in multi-agent systems is extremely fundamental and should be implemented for two reasons: firstly in order to defend systems against threats and attacks, Secondly, its design and analysis in the methodology phase which is ignored.

RESULTS AND DISCUSSION

Integration of security aspects for gna: Since, Multi-Agent Systems (MAS) have grown in popularity, secure communication is of paramount importance. A crucial limitation to MAS is security issues because of the openness of the system. Consequently, a strong mechanism with which agents in our model (GNA) can secure and defend themselves against attacks on other agents and humans needs to be developed and integrated with the main model (Mohammed *et al*., 2012). GNA is a generic nodal approach in which several nodes can be created, for example, human-human node, human-agent node and agent-agent node. Node refers to interdependence entity where a human can collaborate with one or more than one agent via. mediator agent that act as a consultant for its human counterpart.

Basically, number of agents is restricted according to the assignment of mediator agent and delegated tasks that must be achieved. In Fig. 1, (ϕ) represents a human's set of functions and (λ) represents an agent's set of functions. GNA enhanced with security table for each node in the system. A security table store all the information of the node include: node name, agent ID and a secret key which play a role of verification and authentication when nodes interactions occur.

In such a model, appropriate security techniques need to be established by providing the following points:

- A mechanism with which agents in the generic nodal structure can secure and defend themselves against attacks on other agents and/or humans

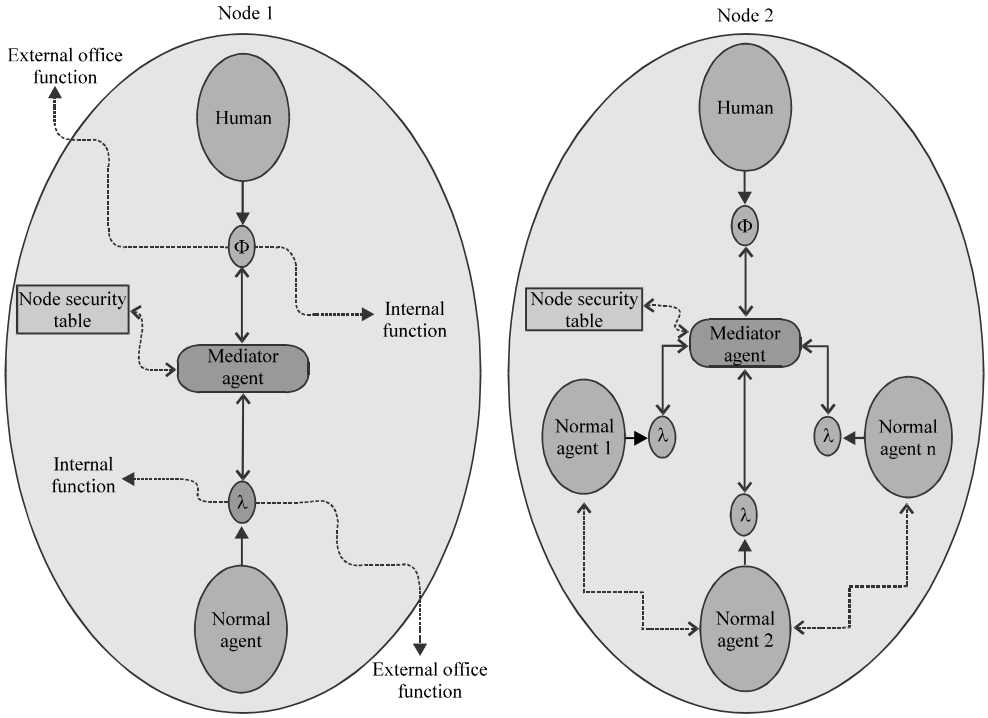

Fig. 1: Nodal approach concept

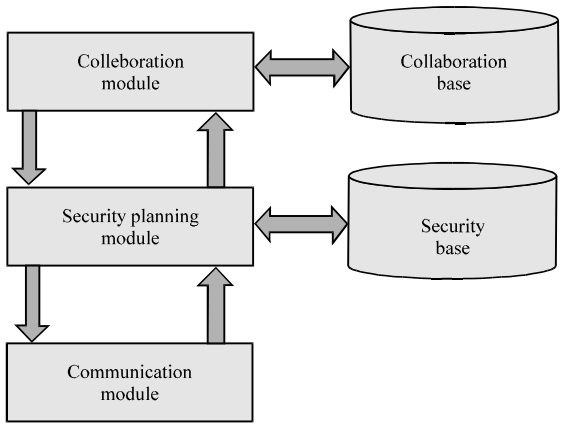

Fig. 2: The architecture for the GNA

- A security infrastructure that is applicable for the model securing agent's actions and communication in general
- Implement security methods for agents in a MAS environment and/or distributed systems and enhance the individual agent's abilities during collaboration

The architecture for the nodes comprises of modules which are shown in Fig. 2. The collaboration module illustrates the cooperative stage between human and agent.

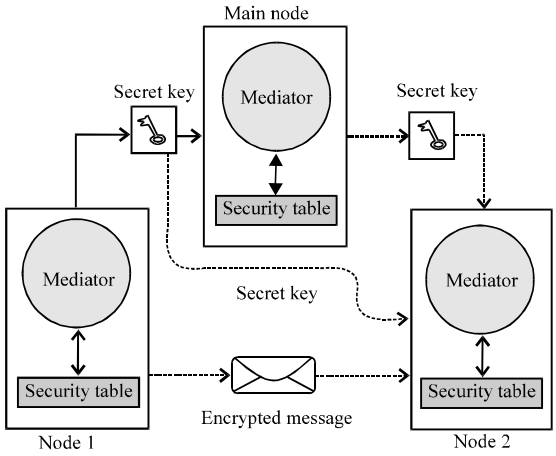

Fig. 3: Security planning module

Communication module provides protocols in which an agent is capability to exchange secured information including cooperative requests and feedback information. The security planning module receives security-resolving requests and decides whether to deal with the request according to the security policy base. Security planning module is detailed further in Fig. 3 which shows how message exchanged between nodes.

Security planning module described in Fig. 3 shows the message exchange among nodes in the GNA.

Specifically when node 1 sends a secret message to node 2 seniors occur before node 2 can open it and read it. Firstly, node 1 sends an encrypted message and to node 2. Simultaneously, node 1 sends also a random secret key to both node 2 and main node to be authenticated latter by node 2.

Note that a verbal node means practically the mediator agent inside the node which has the capabilities and authorities to check and retrieve the information with security table. Finally, node 2 need to send authentication for the main node includes sender node id and its secret key. The main node checks this information if the secret key of node 2 and node 1 are matched then an authentication sends to node 2 and now it can open the received message.

Security in multi-agent systems: Nowadays, a network is considered as a prevalent platform for organizations and people to communicate. The Internet is a manifestation of this network. In fact, netizens deal and communicate with each other via. the internet. However, the internet is highly subjected to be a target of attackers. Intrusion to websites is one of an example of an attack that has rapidly increased and deters some people and organizations from using the internet.

Generally, the current security solutions focus on preventing authorization and authentication access at various systems levels (Wardell *et al*., 2016). Along with this security concern, a great deal of research have been done recently to secure their systems. Researchers in this field attempt to protect the systems from threats that might be caused from inside or outside the organization. Hence, these threats may cause damage to the internet assets as well as to the information.

To overcome these problems, researchers have attempted to provide better techniques by studying multi-agent systems and how the techniques can enhance and improve the security aspects. In particular, a typical security approach in MAS utilizes the software agent abilities and its intelligent, cooperative and autonomous characteristics as well as its collaboration with other agents.

For agent security, the origin of information must be authenticated to protect agents from improperly accessing or communicating with malicious agents (Jansen and Karygiannis, 2000). Additionally, an individual agent should share and permit access to its resources and internal status only with authenticated and authorized agents. Otherwise, the insecure communications among agents as well as between humans and agents could occur. Jung *et al* (2012) show in his study a number of security problems which are caused by various actors. They point out some security causes that impair the entire system such as verification of information, unauthorized access intrusions to MAS, attacks from mobile agents and malicious agents.

Chae *et al* (2016) propose a model for information interoperability systems with security based on multi-agent. They present an agent mutual authentication method in which certificates and session keys are combined. Their MASs proposed for the national R&D information interoperability by providing session keys and mutual authentication method to overcome the security vulnerabilities in MASs. A mutual authentication method is conducted based on certification method where each agent synchronized session keys which are used to propose a method of securing channel.

Researchers have applied the MAS which provides interoperability within and across agent-based applications. They are studying the MAS approach and how the agent-based systems could be improved with better techniques to enhance the security of the systems. Security processes such as encryption, decryption, verification and digital signature are supported when the agents cooperate and communicate together.

CONCLUSION

Lack of comprehensive security techniques to multi-agent systems present a huge drawback. The challenge in multi-agent systems is to provide security mechanisms which do not affect the characteristics (such as collaboration intelligence, dynamic, cooperative problem solving and efficiency) of agents and its performances. Despite the complexities of multi-agent systems, many researchers have attempted to resolve the security problems and proposed various security approaches for MASs. Additionally, they have attempted to improve MAS facilities with security processes to deal with open issues such as secrecy of agent execution. In this study, we have categorized the existing security issues that are applicable to MAS. Among the diversity of security issues, we have devoted our study to review in more detail on threats and attacks in multi-agent systems and how the current security techniques protect message exchanges executions. However, new and aggressive attacks will continue to be released and new technologies will be developed to defeat them.

ACKNOWLEDGEMENTS

This study is supported and financed under Postgraduate Research Scheme Grand (PGRS 160319) from University Malaysia Pahang (UMP).

REFRENCES

Adameit, S., T. Betz, L. Cabac, F. Hars and M. Hewelt *et al*., 2010. Modelling Distributed Network Security in a Petri Net-and Agent-Based Approach. In: Multiagent System Technologies MATES, Springer, Berlin, Germany, ISBN: 13-978-3-642-16177-3, pp: 209-220.

Becker-Asano, C. and I. Wachsmuth, 2010. Affective computing with primary and secondary emotions in a virtual human. Auton. Agents MultiAgent Syst., 20: 32-49.

Bijani, S. and D. Robertson, 2014. A review of attacks and security approaches in open multi-agent systems. Artif. Intell. Rev., 42: 607-636.

Bresciani, P., A. Perini, P. Giorgini, F. Giunchiglia and J. Mylopoulos, 2004. Tropos: An agent-oriented software development methodology. Auton. Agents MultiAgent Syst., 8: 203-236.

Casey, W., J.A. Morales, E. Wright, Q. Zhu and B. Mishra, 2016. Compliance signaling games: Toward modeling the deterrence of insider threats. Comput. Math. Organiz. Theory, 22: 318-349.

Chae, C.J., K.N. Choi and K. Choi, 2016. Information interoperability system using multi-agent with security. Wirel. Pers. Commun., 89: 819-832.

Clark, K.P., M.E. Warnier, F.M. Brazier and T.B. Quillinan, 2010. Secure monitoring of service level agreements. Proceedings of the International Conference on Availability, Reliability and Security (ARES'10), February 15-18, 2010, IEEE, Krakow, Poland, ISBN:978-0-7695-3965-2, pp: 454-461.

Gonzalez, M.C., C.A. Hidalgo and A.L. Barabasi, 2008. Understanding individual human mobility patterns. Nature, 453: 779-782.

Hanna, N. and D. Richards, 2012. A Collaborative Agent Architecture with Human-Agent Communication Model. In: Cognitive Agents for Virtual Environments, Dignum, F., C. Brom, K. Hindriks, M. Beer and D. Richards (Eds.). Springer, Berlin, Germany, ISBN:978-3-642-36443-3, pp: 70-88.

Hornok, S., D. Kovats, T. Csorgo, M.L. Meli and E. Gonczi *et al*., 2014. Birds as potential reservoirs of tick-borne pathogens: First evidence of bacteraemia with *Rickettsia helvetica*. Parasites Vectors, 7: 1-7.

Jansen, W. and T. Karygiannis, 2000. Privilege management of mobile agents. Proceedings of the 23rd National Conference on Information Systems Security, October 16-19, 2000, NIST, Baltimore, Maryland, pp: 362-370.

Jung, Y., M. Kim, A. Masoumzadeh and J.B. Joshi, 2012. A survey of security issue in multi-agent systems. Artif. Intell. Rev., 37: 239-260.

Macal, C. and M. North, 2014. Introductory tutorial: Agent-based modeling and simulation. Proceedings of the Conference on Winter Simulation (WSC'14), December 7-10, 2014, IEEE, Savannah, Georgia, pp: 6-20.

Majid, M.A., 2011. Human behaviour modelling: An investigation using traditional discrete event and combined discrete event and agent-based simulation. Ph.D Thesis, University of Nottingham, Nottingham, England, UK.

Majid, M.A., M. Fakhreldin and K.Z. Zamli, 2016. An enhanced simulation model for complex human pedestrian movement system using hybrid discrete event and agent based simulation. Intl. Inf. Inst. Tokyo Inf., 19: 4213-4218.

Majid, M.A., U. Aickelin and P.O. Siebers, 2009. Comparing simulation output accuracy of discrete event and agent based models: A quantitative approach. Proceedings of the Conference on Summer Computer Simulation (SCSC'09), July 13-16, 2009, ACM, Istanbul, Turkey, pp: 177-184.

Mohammed, K.A., M.S. Ahmad, S.A. Mostafa and F.M.A.M. Sharifuddin, 2012. A nodal approach to modeling human-agents collaboration. Intl. J. Comput. Appl. Found. Comput. Sci., 43: 33-40.

Mohammed, K.A., S.A. Mostafa, M.S. Ahmad and M.A. Mahmoud, 2014. A qualitative analysis of human-agent functions for collaborative multi-agent system. Proceedings of the International Conference on Information Technology and Multimedia (ICIMU'14), November 18-20, 2014, IEEE, Putrajaya, Malaysia, ISBN:978-1-4799-5424-7, pp: 244-249.

Moradian, E., 2013. Security of E-Commerce Software Systems. In: Agent and Multi-Agent Systems in Distributed Systems- Digital Economy and E-Commerce, Hakansson, A. and R. Hartung (Eds.). Springer, Berlin, Germany, ISBN:978-3-642-35207-2, pp: 95-103.

Mouratidis, H. and P. Giorgini, 2007. Secure tropos: A security-oriented extension of the tropos methodology. Intl. J. Software Eng. Knowl. Eng., 17: 285-309.

Mouratidis, H., P. Giorgini and G. Manson, 2003. An Ontology for Modelling Security: The Tropos Approach. In: Knowledge-Based and Intelligent Information and Engineering Systems, Palade, V., R.J. Howlett and L. Jain (Eds.). Springer, Berlin, Germany, ISBN:978-3-540-40803-1, pp: 1387-1394.

Poslad, S., P. Charlton and M. Calisti, 2002. Specifying Standard Security Mechanisms in Multi-Agent Systems. In: Deception, Fraud and Trust in Agent Societies, Falcone, R., S. Barber, L. Korba and M. Singh (Eds.). Springer, Berlin, Germany, ISBN: 978-3-540-00988-7, pp: 163-176.

Ramchurn, S.D., F. Wu, W. Jiang, J.E. Fischer and S. Reece *et al*., 2016. Human-agent collaboration for disaster response. Auton. Agents MultiAgent Syst., 30: 82-111.

Sawa, Y., R. Bhakta, I.G. Harris and C. Hadnagy, 2016. Detection of social engineering attacks through natural language processing of conversations. Proceedings of the IEEE 10th International Conference on Semantic Computing (ICSC'16), February 4-6, 2016, IEEE, Laguna Hills, California, USA., ISBN:978-1-5090-0662-5, pp: 262-265.

Shih, D.H., H.S. Chiang, D.C. Yen and S.C. Huang, 2013. An intelligent embedded system for malicious email filtering. Comput. Stand. Interfaces, 35: 557-565.

Wardell, D.C., R.F. Mills, G.L. Peterson and M.E. Oxley, 2016. A method for revealing and addressing security vulnerabilities in cyber-physical systems by modeling malicious agent interactions with formal verification. Procedia Comput. Sci., 95: 24-31.

Yue, X., X. Qiu, Y. Ji and C. Zhang, 2009. P2P attack taxonomy and relationship analysis. Proceedings of the 11th International Conference on Advanced Communication Technology (ICACT'09) Vol. 2, February 15-18, 2009, IEEE, Phoenix Park, South Korea, ISBN: 978-89-5519-138-7, pp: 1207-1210.