Published in IET Information Security
Received on 22nd February 2010
Revised on 20th May 2010
doi: 10.1049/iet-ifs.2010.0041

Special Issue on Multi-Agent & Distributed Information Security


ISSN 1751-8709

# Distributed security for multi-agent systems – review and applications

*H.F. Rashvand*[1] *K. Salah*[2] *J.M.A. Calero*[3] *L. Harn*[4]

[1]*University of Warwick, Director of Adv. Coms & Editor-in-Chief IET, School of Engineering, Coventry CV4 7AL, UK*
[2]*King Fahd University of Petroleum & Minerals, Associate Professor, Information & Computer Science, Saudi Arabia*
[3]*Universidad de Murcia, Facultad de informatica Campus de Espinado s/n, Espinardo 30100, Spain*
[4]*University of Missouri, Department of Computer Science Electrical Engineering, 5110 Rockhill Road, Kansas City, MO 64110, USA*
*E-mail: h.rashvand@warwick.ac.uk*

**Abstract:** As two major communication technologies, the internet and wireless, are maturing rapidly to dominate our civilised life, the authors urgently need to re-establish users' confidence to harvest new potential applications of large-scale distributed systems. Service agents and distributed multi-agent systems (MASs) have shown the potential to help with this move as the lack of trust caused by heavily compromised security issues and concerns coupled with the out-of-date solutions are hindering the progress. The authors therefore seek new remedies to ensure that the continuity in developing new economies is maintained through building new solutions to address today's techno-economical problems. Following a scan of the literature the authors discuss the state-of-the-art progress followed by some observations and remarks for the researchers in the field. Here the authors recognise the need for new 'distributed security' solutions, as an overlay service, to rejuvenate and exploit the distributed artificial intelligence (AI) techniques for secure MAS as a natural solution to pave the way to enable a long awaited application paradigm of the near future.

## 1 Introduction

Under the new globalisation of the market only companies and organisations that are able to operate promptly, efficiently and globally at all levels can survive the coming tough and competitive business environments. In order to acquire these enabling capabilities, successful companies need to adopt adequately advanced, secure and superior distributed technologies in their working systems as well as the services they provide.

With 50 years of active computing behind us we have seen many innovative uses of it such as controlling critical space missions, to small micro gadgets or smart distributed sensors. One most significant corner stone of the growth that has always been a source of interest is artificial intelligence (AI) [1]. Once AI triggered the dream for a better life by harnessing the computer potentials which would help to reduce humans' tedious labours, and enhance higher precision and hold better control of complex projects. For example, use of AI in the management of complex telecoms networks enabled much useful insight. From the 1990s onwards, with the rapid growth of the internet, however, progress of AI slowed down and its uses were limited to the mobile services.

The internet has naturally shown its own specific way of expansion, puzzling the experts as best characterised by Parkinson's second law: 'systems keep on increasing their complexity as long as being made available'. One part of the puzzle is the user. The question is who are the users? Neither legitimate users nor the legitimate usability of the internet are properly defined anywhere. How could one design a system to be secure against anonymous intelligent users? As long as the access remains widely open and undefined the insecurity can grow faster than its genuine uses. The lack of trust caused by growing concerns in the security witnessed a significant slow down of the internet use in many parts of the globe during the last decade of the 20th century and continued into the 21st century [2].

Many publications indicate that no significant progress is being made on many serious information security issues raised at the start of the century. For example, Qiu and Paterson [3] in their work of modelling vulnerability of information systems indicate that because of mistakes at the time very little progress in the understanding of security problems was being made.

The uncontrollable expansion of the internet has two significant effects on AI. At first it destroyed the well developed traditional network management as a potential user of the AI and second the sporadic trends in a new form of AI resulted in the introduction of a bulky and complex set of new standards instead of an ideal, lightweight, distributed network management. Fortunately, these changes coincided with the time when processors were shrinking rapidly giving a unique opportunity to AI to reappear in a new form of intelligent agent (IA) also called distributed artificial intelligence (DAI).

The break away from traditional AI originated was needed for an agent's autonomy. The agent as a core-independent process has been known for some time. Hewitt's Actor model is a self-controlled, interactive and concurrent process with defined internal states [4]. The multi-agent concept started earlier under the blackboard system, a technique used by the experts to solve complex problems. Further developments appeared using it on the web as a way to collaborate autonomous functions leading later on to form the autonomous agents and multi-agent systems in 2002 and then building the foundation for intelligent physical agents (FIPA) [5]. Since then the multi-agent system (MAS) has been growing to accomplish the early idea of the DAI raising new hopes to enable bringing together scattered applications of the distributed systems.

## 2 Secure MAS

Before reviewing security aspects of MAS and their applications let us have a quick look at some of its basic properties. As mentioned earlier MAS is a loosely coupled distributed autonomous service agents operating under a set of rules and equipped with some common and specific resources to cooperate to achieve specific goals. Each agent performs actions, possesses some knowledge and has some resources at its disposal [5]. They maintain three complementary functions of 'goals', 'self-discipline' and 'communication', independently. The goals characterises the main purpose of an agent required to accomplish the MAS service while the self-disciplinary functions ensure agent's survivability, trust and dependability. The communication functions are required for effective and reliable dialogues between the agent and the core platform, other agents or the outside world. This usually includes security, error control and resource efficiency for which they may use a cross-layer mechanism for better use of scarce resources. Fig. 1 shows a basic model of a single agent of the MAS.

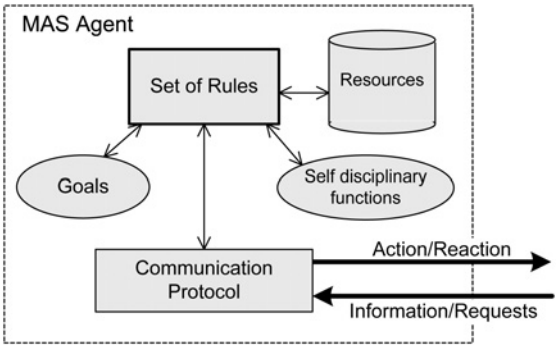


**Figure 1** *Basic model of an agent used in MAS*

Agents of MAS can be similar, complementary or different but they all share some features enabling the whole system to perform. MAS agents differ from stand-alone service agents in the following aspects:

- Control – although they make their own decisions. No agents of MAS can take over control over the system or any agent but they coordinate these tasks with others to achieve the common goals.
- Interaction – agents follow predefined protocols for communication.
- Capability – agents could be different and act differently.
- Environment – decisions are made in cooperation with other agents.

The MAS security services may come in three classes:

- Service-agent protection – security is regarded as one of services provided by the MAS. It can be prioritised or combined in with other services. Normally, agents are protected against external threats through the platform.
- System vulnerability protection – this service protects the platform and legitimate agents from insecure internal processes caused by illegitimate and faulty insecurities.
- Protective security service – the security is regarded as the main goal and implemented through the agents.

For advanced, distributed and complex applications, the usage of MAS should naturally provide most desirable solutions. Stemmed from their natural flexibility they can potentially grow or shrink as required by the highly variable service environment. For the information security applications they are indispensable for reasons of (a) rising level of insecurity because of growing unpredictable threads, (b) a heavy and complex overheads requirement of using classic cryptography methods for distributed applications and (c) serious application bottlenecks because of protocol overheads consuming scarce resources.

As discussed in various parts of the paper, we need to adopt a new distributed approach to address the growing security problem inherited in complex and versatile distributed systems for which we need to clarify a few basic but essential points with regards to relating distributed security to the MAS.

We contemplate that distributed security approach is different to those providing traditional security services to the distributed systems under the Distributed System Security Architecture. For example, a simplified version of the distributed security called 'distributed firewall' is commonly used for protecting private and corporation networks. In this system, host-resident security software treats the network users differently upon a classification into 'reliable' and 'unreliable' users based on their security characteristics rather than their locations.

Like most practical applications the distributed security can also be implemented in an overlay fashion, whereas the security overlay works independently from the application layers although the members of the distributed security could be physically located at the same place which features the suitability of using a distributed approach for securing the MAS. We now provide the following definition for this approach.

*Definition:* A distributed security system represents a set of loosely coupled security members, being an agent or a component, where each member features security autonomy offering a local security service but their findings are shared with other members of the distributed security system.

## 2.1 Multi-agent platform (MAP) security

It is shown that use of a multi-agent style platform simplifies implementation of the MAS. Upon today's software techniques this can be provided through a middleware to facilitate deploying the agents, controlling communication between the agents and maintaining the required security measures for the agents. Owing to their location in the system agents can conveniently handle most of security functions as well as the background processes within the MAS. For example, Fig. 2 depicts a common scenario in which different agents are used to develop a security system within a MAP.

Let us assume that the security system is deployed to handle a distributed intrusion detection system. The processes running the MAP are deployed on different machines. Each agent is in charge of analysing the network behaviour with respect to its own machine while sharing the information on the platform with each other so that they can collaborate in detecting a possible intrusion activity. The information shared among the agents is sensitive therefore the platform should be able to deal with security aspects of agent-to-agent communication for which the National Institute of Standards and Technology proposes different levels of security solutions [6]. For the agent-to-platform security the task is to control the agents. This secures the platform from any possible malicious agent attack. A practical method to achieve this security measure is by means of using a sandbox, defined as a secure execution environment enabling genuine agents to protect the platform against malicious agents. The second level of protection is for platform-to-agent security which is a security service that the platform provides for the agents. Essentially, analogy of this is some kind of privacy computation such as encryption that protects the information associated with an agent against any possible

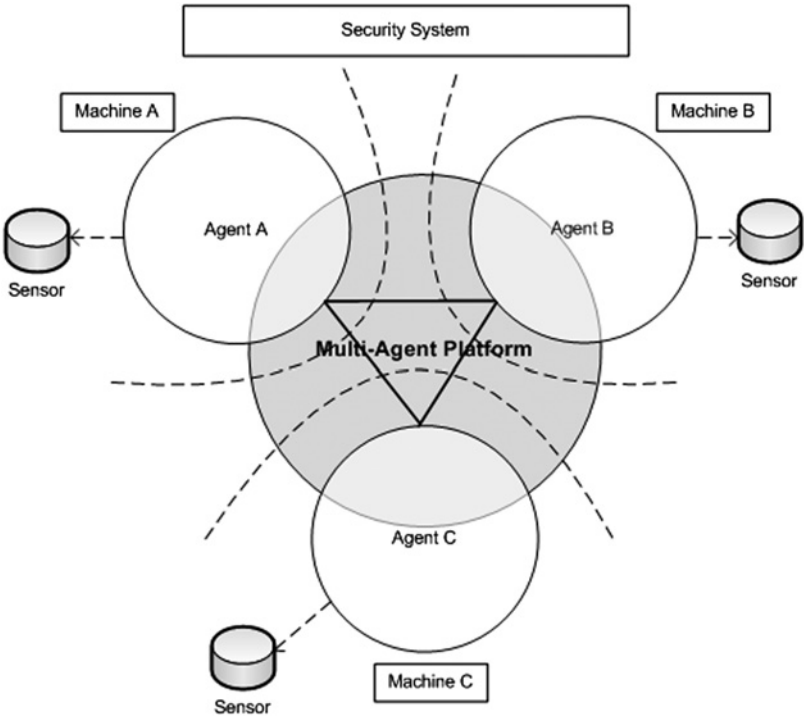


**Figure 2** *Common scenario for deploying security in MAS*




doi: 10.1049/iet-ifs.2010.0041

manipulation such as workflow, privacy and integrity of data. A third level of protection is for agent-to-agent security in which an agent tries to protect itself against actions produced by other agents' misbehaviour such as denial of service, spying or pretentious actions on behalf of other agents. Finally, platform-to-platform security protection is devised for securing interactions between different platforms. In spite its natural capability MAS, however, has not been effectively used in the past to make applications fully secure. For example, experts such as Nguyen *et al.* [7], Poslad *et al.* [8], Mana *et al.* [9] and Garrigues *et al.* [10], clearly point out that lack of proper security is in most MAS applications. One is Aglet (Aglet project page is available at http://aglets.sourceforge.net/ and the latest version was released in 2002), the well-known IBM's platform, which neither provides a security for protecting the agents nor devises any strong authentication and authorisation. It provides a basic user-password authentication process for the platform to identify the agents, which in turn, enables them to access the platform anonymously together with a simple access control based on their two possible roles 'trusted aglets' for agents created by the server and 'untrusted aglets' for agents created by the external servers. Another example is JACK [11], a commercial MAP for building the distributed multi-agent reasoning system [12]. This platform does not deal with any security services and fully relies on Java's internal security. It uses Java security policies for file access control. TuCSoN of Ricci *et al.* [13] is a free open-source MAP and 'S-Moise+' of Hbner *et al.* [14], a middleware that can be used to create structured MAS and Agent Service, by Vecchiola *et al.* [15], a free open source framework for developing MAS, which all lack the provision of strong security measures. They even do not facilitate a proper protection for the agents within the platform and lack a strong protection for the platform against malicious agents. Some do not provide any authentication and some lack security for the communications.

In general, a secure MAP is required to deal with basic security measures such as authentication, authorisation and accounting services plus the usual privacy and integrity of data during the communications. Further requirements for these systems are inclusion of new MAS-based measures such as trust and vulnerability factors. An authentication, for example, located within the MAP can help to protect the infrastructure. A secure infrastructure then enables a protected system as well as protecting agents against malicious processes injected by fictitious agents. Moreover, this approach can also be used as a foundation for authorisation and trust management system. A reliable authorisation and trust management system can enable managing the agents' privileges and control their behaviour as well as maintaining their privacy. For providing a secure MAP, JADE [16], well-known development framework for an agent in Java, then extended into JADE-S [17] now comes with more recent developments of SAgents [18] and ExJADE-S [19] enhancing the security aspects of the platforms. All of these extensions incorporate strong authentication systems adopting certificate management, a distributed access control mechanism and an accounting system. They also require keeping a track on agents' behaviour while maintaining data integrity, trust management, encryption and confidentiality of the communications.

Ismail [20] proposes a method to tackle addressing security issues of a secure MAP directly. In this method the platform implements a transparent authentication integrated within the authorisation service. The system supports a dynamic exchange under the evolutionary access rights and claims modularity, portability, non-repudiation and high performance. It uses a digital signature for authentication of the agents and a new algorithm to control the exchange of access rights among the agents.

Fernandes *et al.* [21] combine the peer-to-peer networking features to build a secure MAP. This platform offers a strong authentication service based on X.509 certification enhanced with authorisation, secure transport and secure execution for the agents. The platform consists of an overlay network by means of a distributed hash map, called Pastry network, being used to distribute the security services across the network. Owing to the nature of the overlay network this platform can also provide a fault-tolerant environment for all agents, a desirable feature in a secure critical system.

In order to secure the communication in existent insecure MAPs, the X-System [22] provides different security architecture. In essence, the secure communication and authentication is by means of a public key infrastructure based on the extension of the FIPA [23] protocol. This well-known inter-operation protocol shares messages between the agents and the MAPs thus, providing FIPA compliant security architecture for the MAP.

## 2.2 MAP security developments

Considering that secure MAS platforms offer enhanced efficiency and reliable performance, they can be effectively used for securing complex distributed systems. Two trends for developing new distributed security models are most significant. One is to develop the existing MAS platforms for further strengths in their security capabilities whereas the second trend provides an overlay for the existing platforms and then develops whole new brand secure platforms.

For the first approach, Shakshuki *et al.* [24] provide a detailed and comprehensive description of the MAS including security services, prototyping and implementation of the platform. Fig. 3 shows this architecture which is composed of four layers: (i) interface layer for the human-system interaction, (ii) authentication layer for authenticating users of the platform, (3) authorisation layer for controlling access to the services and information resources and (4) service layer in charge of providing the

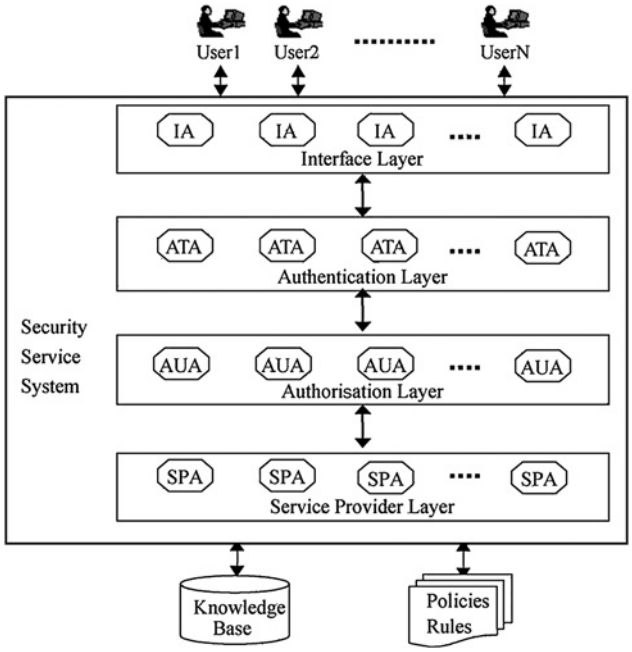


**Figure 3** *Multi-agent architecture for secure services*

architectural services. So, each layer contains several agents in order to offer the services associated to the layer and to carry out these services in a scalable and distributed way.

With regard to the authentication layer, MAS enables the usage of cloud and grid computing that multiple user applications should manage for users belonging to different organisations. Fugkeaw *et al.* [25] propose an authentication approach for enhancing the existing MAS application scenarios for design of the secure MAS. This, in effect, can be viewed as a multi-agent public key infrastructure (PKI) authentication scheme that contains several authentication agents coming together for an action when a new client request appears. As all agents are responsible for a whole set of validating the certificate request, granting access roles to the clients and controlling a smooth concurrent use of the applications a secure cooperation between the MAS agents is essential for maintaining the service. This approach also can support the single sign-on feature service among all other applications for all users within the environment.

For the model authorisation layer, Fugkeaw *et al.* [26] provide a distributed role-based access control method for multi-application scenarios with multiple users and multi-relying party federations. The agents use a public key infrastructure and a privilege management infrastructure to provide the authentication and authorisation services. To encourage a fair distribution, a better scalability and higher performance, as well as ease of management and extensions, the multi-agent concept is applied in the automation of most processes such the authentication, authorisation and accountability functionalities as well. Finally, they can foster usage of the certificate trust lists to produce different PKI domains that can inter-operate more effectively. Likewise, we can also name another use of multi-agents authorisation scheme for medical systems, MedIGS [27]. This authorisation scheme can be used for complex systems responsible for integrated multiple hospital services, each with its own security system where agents provide a mapping of the security information across all the system providing interoperability services among them.

Other security systems suitable for further development under the MAS are the distributed intrusion detection systems. The architecture of these systems is similar to those previously mentioned in association with Fig. 2. In this context, Mosqueira-Rey *et al.* [28] devise a method equipped with a misuse detection agent. This is one of the distinct agents in a multi-agent-based intrusion detection system which has been also implemented in a JADE platform. The agent analyses the packets in the network connections using a packet sniffer and then creates a data model based on the collected information. This data model is input to a rule-based inference engine agent, which uses the Rete pattern matching algorithm for applying the signature-based intrusion detection system's rules, Snort.

Another multi-agent approach for securing the intrusion detection comes from Ou and Ou for a danger-theory-inspired artificial immune system, MAAIS [29]. The best analogy for this method is that each agent coordinates with the others to calculate a danger value for the system. It then produces an immune response for the malicious behaviour activated by either the computer host or by the security operating centre. It is worth mentioning that the security operating system is an element in the architecture of this proposal intended to be used for coordinating the information provided by different agents.

For severe security cases, Szymczyk [30] fosters a multi-agent security system for detecting bots, to prevent troubles coming from common computer attacks sourced from hackers or systems being infected by malicious software and used for illegal activities. This method uses a hybrid style of host intrusion detection system with an operating system event log analyser. The detection algorithms of this proposal are based on the signatures derived from analysing various groups of malicious software known to create bots.

## 3 Secure MAS for e-commerce and e-business

Assuming a security enabled MAP being the key process for secure MAS applications let us look into some application scenarios. Interested reader can find more details on current state-of-the-art and potential application scenarios of MAS in Tweedalea *et al.* [31] and Pechoucek and Marik [32].

The internet has emerged as a global infrastructure to be used for commercial and business applications, also called




doi: 10.1049/iet-ifs.2010.0041

e-commerce and e-business. In e-commerce, the main activities consist of online bidding, online buying and selling of items, online trading and online banking commonly used for typical services. Ideally, e-commerce and web services promise to make the businesses feasible upon a usable internet access by anyone, anywhere, anytime and over any platform [33, 34]. However, the access to high-speed internet has shown to be only one part of story. In practice, potential services require tight security measures. Although a heavily controlled use of resources under limited closed community access over virtual private networks can be secured using the traditional methods but in no way this approach can be accepted as it will compromise the global market conditions and slows down the progress. The alternative fertile approach for a true open economy, however, imposes security sensitive issues associated with 'open access' and 'system complexity'.

In such condition the massive unknown users accessing the system with even a small degree of illegitimacy process could drop the trust down to the floor and perish any potential applications. Basically, as the service spreads over less secure locations by different systems and users, the number of information security attacks and associated incidents such as identifying theft increase [35, 36]. This is due to the fact that all these transactions require, to some degrees, disclosure of private and sensitive information between users and the service performs to allow the access and provide the online service. Such information could be a customer's social security number, mailing address, email address, identity information and credit card details. None of the above-mentioned private information details can be risked or compromised at any cost, to be seen or accessed by any unauthorised systems or users. All these sensitive details need to be protected from any immense proactive insecurity actions being an intrusion, interception or disclosure of data during the exchange or stored in a database.

Without any rigorous and strong security measures in place for any of these services, there will be little confidence and trust between the service providers and consumers of the e-commerce, thereby jeopardising the existence of the e-commerce industry with the possible devastating financial impacts which may result in moral consequences and lack of confidence on the e-commerce consumers. In an e-commerce environment, sensitive data travel across distrusted media manipulated by numerous distributed entities [37] and if in any part of the processing chain something gets compromised, the entire security system breaks apart [34].

Current security solutions use traditional methods and focus on securing the network and transport layers by employing network security appliances and protocols such as firewalls, proxies, IDS, and IPSec, SSL and TSL protocols [37]. Most e-commerce and web services operate at the application layer and exchange data as the communication protocols providing the service dictates they must be secured and protected all the way from one end to the other with request for a reply [37] so the application service should withstand any possible attacks at every stage of the transaction [38]. A more serious part of the problem is that once in place the attackers can easily adapt themselves and become more sophisticated, using variable parameters and continuously pressurising the traditional security users to take on extra measures. As a result many applications grow rapidly in cost and overheads so that they become too complex to run efficiently or take the risk. The list of attacks is growing longer every year as they become more cunning and difficult. Examples are unauthorised access, unauthorised alteration of message, replay and man-in-the-middle.

In order to prevent secure services from such sophisticated threats we may seek the answer in a better use of the intelligence. That is, in order to be able to secure our future complex distributed application, adoption of new superior intelligent security mechanism is becoming essential. It is therefore not surprising to see that a number of security solutions based on MAS have been developed for securing e-commerce and web services. In such a solution, if one agent cannot posses all the information required to identify a malicious activity by itself the agents should cooperate with another one and reach a collective decision against the security breach.

Pedireddy and Vidal [39] provide a solution by building up such a cooperative system between the agents at different network nodes to enable the system to communicate to protect the system. Here, the cooperative agents determine if suspicious events are part of a distributed attack and, if so, warn other agents about the possible threats.

Another solution is to adopt agents for e-commerce, to handle trust, security and legal issues. Fasli [40] discusses trust aspects of the security issues and how trust can be addressed through the use of cryptography. Gorodetski and Kotenko [41] propose a scheme whereby, in order to reach an effective defensive state against network attacks, an aggregate of overall behaviour for the system is constructed by means of local interactions among local software agents. The software agents are then used to perform multiple tasks by gathering information from different sources, operating a fuzzy or probabilistic knowledge, forecasting intentions and actions of the opponents, estimating possible risks, trying to deceive opponents and reacting on opponent actions. A conceptual model has also been developed to capture agent's behaviour and generate a cooperation device for an effective counter measure against attacks. The security effectiveness of such a system has been achieved through the simulation.

Moradian and Hakansson [38] use a meta-agent overlay in their MAS application. It monitors, audits and controls the message paths, starting from initial sender via intermediaries to ultimate recipients. The primary role of a

meta-agent system is to perform a reasoning function and then devise a plan of action prior to making any major decisions [42]. In this method the extracted knowledge from the ground agents is used for controlling their behaviour. These ground-level agents are called information gathering agents who report any possible attacks back to the meta-agent in which decisions can be made. As shown in Fig. 4, the ground-level agents detect all aspects that are relevant to the choice of action and have access to all information about IP addresses, protocols, servers, routers and any components involved in the message passing. The main responsibility of meta-agents is to avoid inappropriate routes in the network. That is, although the ground agents move around the network holding their messages, the meta-agents consider the circumstances at a given time and act upon any unexpected behaviour or events. All events are reported to the meta-agents. Specifically, the agents follow the messages from one network element (e.g. a router) to another so that the route segment in between them is determined. The meta-agent can declare an unauthorised routing segment has occurred, and order the ground-level agents to halt further operations and actions.

One interesting research area of e-commerce security is examining consumer's perception of risk and trust. As mentioned in various parts of this paper, lack of trust always leads to reduced customer confidence in getting engaged in any e-commerce activities [43]. Zhao *et al.* [44] propose a scalable trust model for e-commerce. The model is based on establishing trust through a mediating agent to perform a transaction between a buyer and a seller so that a successful and secure e-commerce service is achieved. Given a set of transactional or mediating agents, the question is how to find or select the most trustworthy agent to take responsibility over execution of the transactions between a buyer and a seller. The above authors demonstrate that their trust model is capable of providing a degree of assurance to the customer with respect to the exchange of sensitive information carried out between the customer and the e-commerce provider.

Karygiannis and Antonakakis [45] analyse the security and privacy issues of the e-commerce and provide some security guidelines for a secure MAS location-aware e-commerce. They also explore various combinations of mobile commerce (m-commerce) and location-aware services for online and offline bricks-and-mortar services.

Alagar *et al.* [46] introduce security agents to e-commerce platforms comprised of multiple intelligent cooperating agents. They show how to add the security attributes to the system and how to present guidelines for incorporating security policies in such a platform. Security agents use a knowledge base for the security and business rules to detect activities that may violate business workflow policies. As shown in Fig. 5, the security agent is a watchdog process that monitors the activities of agents in the system. It has access to the agent state logs, events of accessing sensitive data and the timing information. The security agent defines the boundaries and sets the plan of action to help to identify security breaches and malicious activities. Interference actions are analysed using data mining techniques for extracting the required knowledge from large piles of data and logs. In this method, if it infers that some agents involved in a business transaction are not legitimate or that the data they share violates security and business rules the security agent has the right and ability to interrupt a communication or a service. In short, the primary function of these security agents is to ensure that every message is acted upon in the system in agreement with security and business policies governing the transaction.

Another security issue in the e-commerce arises upon the recommender systems [47, 48] which suggest provision of customised recommendations to the customer about the services and products; shopping agents should guide customer during their sessions; and middle agents should be used for acting on behalf of the customer upon their decision, for example, for bidding automatically in an auction [49]. Shi *et al.* [50] provide a new bidding auction protocol based on MAS with bid privacy in which the deal is simulated including hazards such as data attack and denial-of-service attack, anonymity disclosure, collision between customers and a certain supplier, among others.

Finally, further critical issues in securing e-commerce agents from malicious agents can be found in various literatures. For example, Marques *et al.* [51] identify three protection kinds in e-commerce. Hosts should be protected

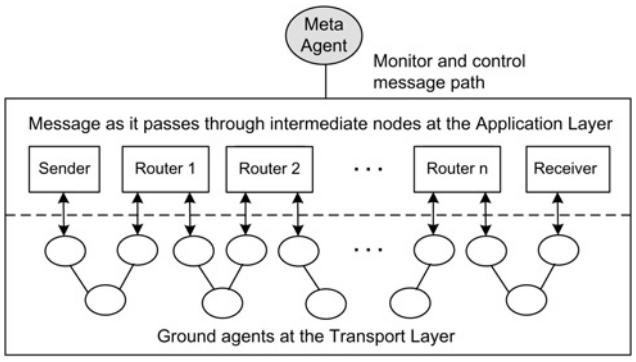


**Figure 4** *Role of meta-agents in securing and controlling messages in transit [38]*

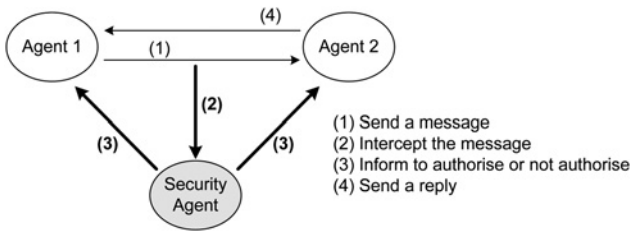


**Figure 5** *Role of Security agent in an e-commerce platform [46]*




doi: 10.1049/iet-ifs.2010.0041

from malicious agents, agents should be protected from other agents and agents should be protected from malicious hosts. The details of all these three protection types are described in the security mechanism.

## 4 Secure MAS e-health

Recent advancements in IT have promoted a significant growth in the healthcare industry. Healthcare applications typically require loosely coupled heterogeneous components, a dynamic and distributed management of data and remote collaboration among diverse entities and users [52–54]. The agent approach has shown a potential to be deployed in a wide range of applications in health care services. Agents can maintain the autonomy of the collaborating participants, integrate disparate operating environments, coordinate distributed data, such as patient records held in different departments within a hospital or in several hospitals, clinics and surgeries [54], improve patient management through distributed patient scheduling using some co-operating intelligent agents, provide remote care monitoring and information for groups such as the elderly and chronically ill, undertake hospital patient monitoring, supply diagnosis decision-support and enable intelligent human computer interfaces to adapt to medical data upon users requirements.

The e-health systems normally require handling of a very sensitive large amount of medical data. These include patient's medical history, diagnosis, test results and various personal details. Therefore all usual properties such as classic confidentiality, authentication, integrity and non-repudiation should also be guaranteed in any agent-based health-care system. The use of cryptographic methods is also important to protect the access to data while it is being transmitted among agents. Li and Hoang [55] propose a role-based access control scheme to protect confidential e-health data from unauthorised access. The proposed scheme is dynamic in terms of the interactivity between three main elements defined as: role, interaction and organisation. The e-health system is perceived as MAS with different personnel playing different roles, requiring varying interactions among themselves, under different organisational contexts. The role is defined as a peer-to-peer model, capable of receiving requests from other roles as well as initiating requests to other roles of the system. A role that initiates a request to another role is defined as an initiator role. The role that receives a request is called a 'reactor'. Each role is associated with a security property or a dependency, which defines the constraints to ensure successful satisfaction of the dependency. These constraints represent a set of conditions that restrict or allow the entities belonging to a particular role for performing a certain task, such as data access.

Another common health-care application area in which security can play a significant role is the information management. MADIP [56] project uses a MAS architecture for supporting the intensive and distributed outpatient wide-area monitoring applications. The architecture is designed to perform under a continuous long-term health monitoring without interfering with the patients everyday activities without restricting their mobility. SAPHINE [57] is a typical application of MAS that can be used for monitoring patients remotely at their homes as well as in the hospital. These projects could save both governments and patients significantly and reduce the load and time of medical practitioner, patients, beds, nurses, space etc. Both projects are using secure MAS platforms.

Another recent secure MAS application framework has been presented by Sulaiman *et al.* [58]. This framework, suitable for secure clinical applications, uses the multi-agent approach. The architecture deals with different types of actors and communications providing security accordingly. In essence, the information access is controlled using an authorisation system according to the actors (nurse, doctor, device, social worker etc.). The framework defines various levels of sensitivity for the communication. Levels are labelled in 1–5, for being extreme, high, medium and low sensitive and public. For example, doctor-to-doctor and doctor-to-patient communications could be considered as extremely sensitive whereas social worker-to-doctor could be medium sensitive.

Health Agents [59] is another typical MAS application that makes use of a secure multi-agent framework to secure the decisions made on sensitive medical data. It provides a support system in a clinical environment to help determine the diagnosis and prognosis of brain tumours. This framework provides a security model based on role-based access control.

## 5 Secure MAS system control

Another important application area of secure MAS is in controlling critical systems. For example, OCA system [60] which is designed by NASA uses the MAS approach for carrying out their space mission control. This system is in charge of file management in the communication system of the International Space Station. Owing to the nature of the content of data being transferred the security aspects of this system become critically important. In order to secure the communications in the system it uses the SSL transport in which for their cryptographic requirements they adopt the Federal Information Processing Standards Publications 140–24 (http://csrc.nist.gov/publications/_ps/_ps140-2/_ps1402.pdf).

The vehicle traffic control is another control application area where security is important. For example, ABRTTDMS [61] is agent-based real-time distributed traffic detection and management system implemented using the Mobile-C MAP. Mobile-C MAP supported by secure communications and strong authentication based on X.509 certificate which also provides a privilege authorisation management. This system makes use of a

security agent called agent security manager responsible for maintaining security policies for the platform and its infrastructure.

We have seen an interesting increase in the use of security systems for controlling the video sensors in surveillance and vigilance systems over last few years. For controlling simultaneously various tracks in many locations this system uses a distributed security model capable of sharing information among peer agents for reaching scalable solutions. In this context, Patricio *et al.* [62] describe a secure multi-agent framework for the visual sensor networks. They use the MAS in order to coordinate camera-based video surveillance. The idea is to embed a software agent in each camera in order to control the captured parameters. Then coordination is based on the exchange of high-level messages among agents. Agents use an internal symbolic model to interpret the current situation using the messages from all other agents to improve global coordination.

Owing to the sensitive nature of managed resources such as the electric power the power plant management can be regarded as good application of secure MAS. A good example is GridAgents [63] which adapts a JADE MAP for controlling distributed energy applications. This platform has been used in a trial deploying resource-controller agents in Australian electric power grid infrastructure. The platform provides a real-time two-way communication enabling decision making for the distributed energy resources in electricity distribution networks. The value-added requirement of this approach is beneficial to the network operation by alleviating the effects of peak wholesale prices and network constraints. This platform relies on the security services provided by the JADE security extensions.

## 6 Secure MAS network management

These days, security is an integral part of network management services but because of its long history we see a huge diversity in the security aspects of network management. The IEFT (Internet Engineering Task Force (IETF), online) has published a set of standards and RFCs related to securing the network and information. However these standards are not MAS based hence because of their lack of capabilities cannot adopt offer secure MAS or can do but at the cost of considerable extra complexities. Furthermore, the fabric and infrastructure of new network applications inherently match secure MAS make them suitable for the integration of network management with distributed security models.

In order to help with the development of robust and highly adaptable communication systems, NEC has recently released a system that is a combination of a 'distributed agent-based system' and a 'reconfigurable peer-to-peer overlay network' [64]. One of the challenges of this new development is that this system is tested against particular scenarios whereby the environment is dynamic and rapidly changing with adverse conditions as those to military systems. In such environment, it is hard to guarantee the security of communications.

Similarly, for a highly competitive business environment, Das *et al.* [65] prototype an integrated data centre power management solution based on MAS that includes server management tools, sensors and monitors, in addition to an agent-based approach in order to achieve certain specified power and performance objectives. The results show that by cleverly turning off some of the servers under low-load conditions, they can claim over 25% power saving over the unmanaged case where there are no incurring SLA penalties for typical daily and weekly periodic demands seen by the Web server farms. In such systems, security has been taken into account as misuse agents that can cause denial-of-service attacks to services provided by the data centres.

Another network management distributed security development from Wang *et al.* [66] where an 'immune MAS' is used to provide network intrusion detection. Their experimental results exhibit that this system not only reduces effectively the rates of false-negative and false-positive but also it can adapt itself to a continuously changing network environment. Similarly, Holloway *et al.* [67] propose an effective and more efficient self-organised entangled hierarchical architecture comprised of multiple agents that decentralise the network security controller. In this case, it is used as an evolutionary approach based on swarms behaviour for which a desired network security is defined, formalised and enforced by the means of collaborative interactions with other agents.

## 7 Secure MAS military application

The intrinsic nature of the military application scenarios requires the systems to deal with security as a top priority factor. In effect, secure MAS can provide key security features and services in such scenarios. Beautemen *et al.* [68] discuss detailed key factors that need to be taken into account when provisioning applications, tools, devices and infrastructure for military domain in the context of autonomous agents and MAS.

A military application scenario of secure MAS is the use of critical decision making support systems in hostile environments to help in military tactics and military combat actions in the battle field. Cila and Malab [69] provide a secure MAS architecture which matches the needs of future multi-dimensional warfare. This is a two-layer multi-agent architecture in which the first layer contains mission analysis agents, mission time scheduling




doi: 10.1049/iet-ifs.2010.0041

agents, enemy situation analysing agents, own situation analysing agents, logistic agents and action generating agents. The agents need databases for the intelligence, environment, terrain, enemy tactics, techniques and procedures, own tactics, techniques and procedures and logistics information. Fig. 6 depicts the architecture for this military scenario in which all the databases and agents are interconnected by means of the security services provided by the secure MAS. Owing to the nature of these systems, the second layer of this architecture is a simulator tool in which all these agents can be intensively verified and validated before getting the system ready-to-use in the real battle field.

Mine detection is another common military application which requires secure MAS. For this application Manzoor *et al.* [70] propose a multi-agent-based model for detecting mines in an unknown environment. As the positions of mines are unknown and their locations cannot be predicted using classic probabilistic methods, the use of secure and distributed agents can be very effective. Such agents can carry mine detector devices and coordinate their actions and movements with each other for the best result.

Most mission-critical scenarios, being a military or disaster recovery, often call upon formation of coalitions, made up of people from different countries or organisations to adhere to certain policies. These policies define explicit obligations, permissions and prohibitions governing members of the coalition. In such scenarios, planning a joint action can be very complex because of many factors involving human planners, policy constraints and conflicts that may exist between the policy makers. To alleviate such complexity, Burnett *et al.* [71] propose a solution that utilises secure MAS in which agents support human planners in coalitions in order to support coalition mission planning under such policy constraints.

For bio-defence application scenarios, Carley [72] describe a secure MAS for simulating bio-attacks considering many factors which include evaluating response policies, data efficacy, attack severity and detection tools are required to identify weaponries for biological attacks in the presence of background diseases such as flu. Owing to the critical response time requirements, the MAS may need to use a large number of computing resources which may function over diverse domains.

It is also important to note that secure agent and secure MAS methods can be extremely useful in offering new means for designing military medical command systems. They enable new open, flexible, heterogeneous and dynamically evolutional capabilities for the system. Xu *et al.* [73] analyse the functional and performance requirements of strategic level architectures for military medical service command system. Agent-based strategic physical architectures and hierarchy of military service command system work together to implement secure MAP for best use of key technologies.

## 8 Trends and research guide

There is a growing need to develop better integrated agent and multi-agent technologies to meet the increasing demand for new dynamic distributed applications over emerging mix internet–wireless media. As mentioned in various parts of the paper many application scenarios have

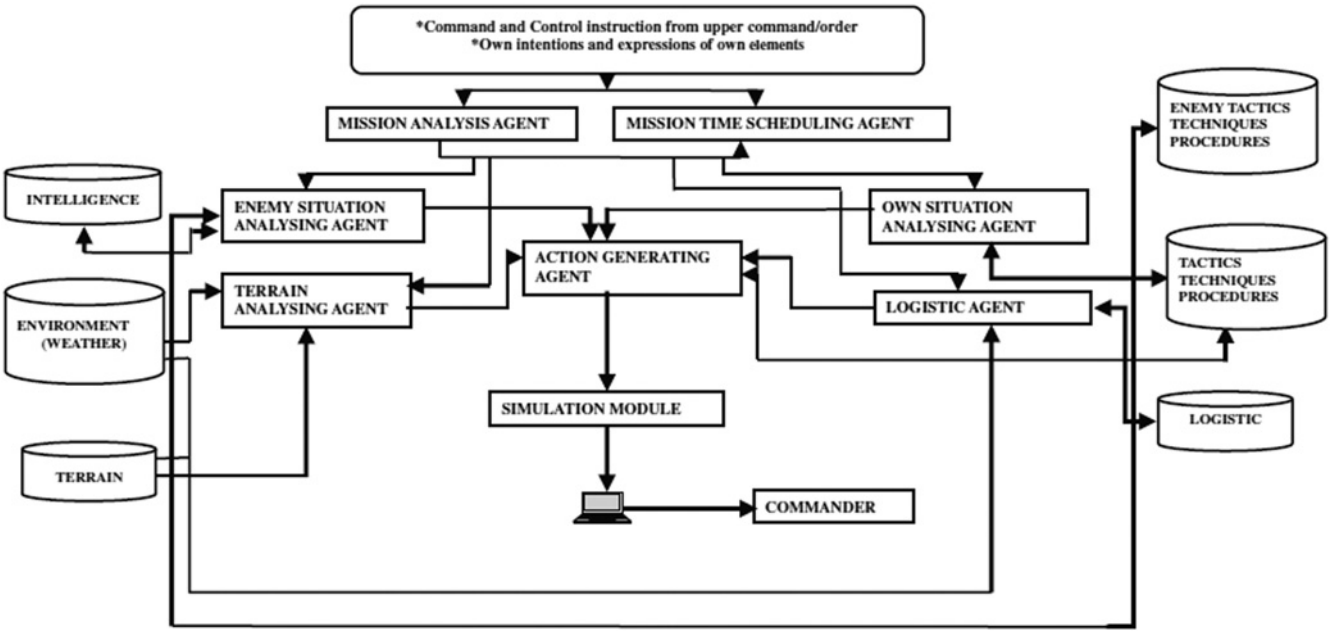


**Figure 6** *MAS architecture to support critical decision making in the battle field*

already started to build upon the dynamics of secure MAS. This is due to three major upcoming trends:

1. successful applications require certain dynamics which simple systems cannot provide,

2. majority of emerging application scenarios are distributed in nature,

3. insecurity problems are hurting new technology-based economies and despite its continual efforts at massive expenses the traditional security systems fail to build adequate trust required to attract potential applications upon heavily invested ICT infrastructure.

Stemmed from distributed intelligence, therefore it is natural to consider secure MAS, as the best trend to build new solutions, superior over the classic methods. Owing to their natural superiority, empowered by parallel processing and distributed computing environment, MAS can enable individual and teamed up agents to coordinate, collaborate and gather optimally managed distributed information for holistic views of the overall system's behaviour, provide upmost knowledge and deliver most resource-efficient service upon precise collective decisions. For example, in most secure applications the individual agents need to communicate and share information with other to determine the existence of certain suspicious activities events or as part of their normal activities they share various security information with other agents, for example, warning each other about possible threats. The real progress is, however, just beginning to emerge so we have very little results to show on the real benefits of the distributed security models and associated distributed intelligence. MAS is expected to grow and we anticipate seeing further progress in secure MAS-based developments.

For a start we need new developments for security tools where we can establish more sophisticated measures for emerging technologies and harness secure MAS enabling techniques to address two key security issues. First, MAS must be able to provide the security using agile and cost-effective mechanisms to ensure all classic security requirements as 'confidentiality, integrity, reliability and availability of information where ever on the globe' capable to identify and mitigate known and new upcoming possible security issues. Second, individual agents can communicate securely with each other and able to monitor, identify and control any malicious, intrusive and suspicious activity. The new massively multi-agent systems approach is emerging with a potential to promote a new dependable design paradigm for implementing ubiquitous computing and ambient intelligence. For this millions of electronic devices with computing facilities in public spaces are interconnected in *ad hoc* style and behave coherently. The architectures used in such a large-scale distributed system need to come with some key features: (a) network composition capability, that is, supporting on-the-fly negotiations and agreements across different administrative domains and (b) self-managed capability for automatic reconfiguration.

Further research activities also required for securing the ubiquitous networking and ambient environments. We need well secured agents to adapt themselves with the dynamic users: location, context, platforms and associated architectures. Compositional adaptation and learning of individual and team agents needs new ways to allow the MAS agents to change their behaviour and have reconfigurable structure, timely and radically.

Immediate research avenues are expected to increase in securing the cloud and grid computing. In cloud computing, data and computing resources are typically distributed over a large geographical area and exist off the users' premises where computing resources are elastic and dynamic.

The new security solutions are also required for individual agent's roles in the use of information in various disciplines. Data fusion, ambient intelligence, pervasive and ubiquitous computing, cloud and grid computing, services oriented computing, semantic web, ubiquitous access are also associated with the new secure MAS application paradigm.

## 9 Conclusions

Considering that the amount of investment in computing has been growing faster than most other industries, it is disappointing to see so little has been accomplished to secure our valuable systems and private information.

One potential new development is a distributed approach to the security that could begin with secure MAS which has been around for some time but progress has been sporadic, sluggish, disjointed and far from perfect with a serious lack of harmonisation, and we may only articulate we have seen only top of the iceberg of what secure distributed systems can offer.

Based on our review we have discovered two closely inter-related trends for developing new solutions: (i) secure MAS, where we seek new solutions for securing the general purpose MAS applications and (2) security MAS, as a new overlay security solution in which we propose distributed security models, to adopt MAS approach for securing distributed systems. The following points may help researchers to focus a better directivity in this research avenue:

- New developments for promotion of new services such as 'multi-agent security service'.

- Promotion of cross-layer optimisation to revolutionise ICT under secure-MAS to overcome existing distributed systems bottlenecks.


*IET Inf. Secur.*, 2010, Vol. 4, Iss. 4, pp. 188–201

doi: 10.1049/iet-ifs.2010.0041

• Enable the adaptation of information security under distributed intelligence and IA for distributed security solutions.

• Create a trustworthy model to enable us analyse the 'trust impact factor' which can be used to measure systems' insecurity, as presently trust is not well defined as an engineering tool and is rarely applied in the security systems.

• We noticed the proliferation of secure MAS in diverse security functions such as authentication, authorisation, accounting, intrusion detection system, log analysers, malware and botnet detections. New models of secure MAS can be extremely useful in developing new security systems for distributed application scenarios.

• The design of an efficient method to tackle 'context-aware security' in which the mobile agents are able to deal with security according with the context in which the agents are running.

• Enhancements in self-management capabilities of MAS and secure MAS for better self-management and self-protection capabilities as required to enable massively untouched potentials of distributed systems.

• Improve countermeasure techniques for agents and MAS to protect system infrastructure against attacks.

## 10 References


[1] MINSKY M.: 'Steps toward artificial intelligence', *Proc. IRE*, 1961, **49**, pp. 8–30

[2] BORGAN J.S.C.: 'Trust agents' (John Wiley, 2009)

[3] QIU X., PATERSON R.: 'An innovative network security vulnerability modeling method and tool', *IEEE Commun. Mag.*, 2010, **48**, pp. 104–108

[4] HEWITT C., BISHOP P., STEIGER R.: 'A universal modular ACTOR formalism for artificial intelligence', *Proc. of the 3rd International joint conference for artificial intelligence*, 1973, pp. 235–245

[5] FASLI M.: 'Agent technology for e-commerce' (John Wiley, 2007)

[6] KARYGIANNIS T., JANSEN W.: 'Mobile agent security', Technical Report NIST SP 800-19, National Institute of Standards and Technology, 1999

[7] NGUYEN G., DANG T.T., HLUCHY L., LACLAVIK M., BALOGH Z., BUDINSKA I.: 'Agent platform evaluation and comparison', Technical Report 5FP 1st-2001-34519: Institute of Informatics, Slovak Academy of Sciences

[8] POSLAD S., CHARLTON P., CALISTI M.: 'Specifying standard security mechanisms in multi-agent systems', AAMAS 2002, in FALCONE R., BARBER S., KORBA L., SINGH M. (EDS.): 'Trust, reputation, and security: theories and practice', Springer Verlag (2003), pp. 227–237

[9] MANA A., MUÑOZ A., SERRANO D.: 'Towards secure agent computing for ubiquitous computing and ambient intelligence', *LNCS Ubiquit. Intell. Comput.*, 2007, **4611**, pp. 1201–1212

[10] GARRIGUES C., ROBLES S., BORRELL J., NAVARRO-ARRIBAS G.: 'Promoting the development of secure mobile agent applications', *J. Syst. Softw.*, 2010, **83**, (6), pp. 959–971

[11] AOS: 'Jack intelligent agents: Jack manual'. Technical Report, Agent Oriented Software Pvt. Ltd, 2005, release 4.1

[12] D'INVERNO M., LUCK M., GEORGEFF M., KINNY D., WOOLDRIDGE M.: 'The dMARS architechure: a specification of the distributed multi-agent reasoning system', *J. Auton. Agents Multi-Agent Syst.*, 2004, **9**, (1–2), pp. 5–53

[13] RICCI A., OMINICI A., DENIT E.: 'Enlightened agents in tucson'. AI*IA/TABOO-Workshop dagli Oggetti agli Agenti: tendenze evolutive dei sistemi software (WOA), 2001

[14] HBNER J.F., SICHMAN J.S., BOISSIER O.: 'S-Moise+: a middleware for developing organised multi-agent systems', *LCNS Coord. Org. Inst. Norms Multi-Agent Syst.*, 2007, **3913**, pp. 64–78

[15] VECCHIOLA A.G.C., PASSADORE A., BOCCALATTE A.: 'Agentservice: a framework for distributed multi-agent system development', *Int. J. Agent-Oriented Softw. Eng.*, 2008, **2**, pp. 290–323

[16] BELLIFEMINE G.C.F., POGGI A., RIMASSA G.: 'JADE: a software framework for developing multi-agent applications. Lessons learned', *Inf. Softw. Technol.*, 2008, **50**, pp. 10–21

[17] VILA X., SCHUSTER A., RIERA A.: 'Security for a multi-agent system based on jade', *Comput. Sec.*, 2007, **26**, pp. 391–400

[18] GUNUPUDI V., TATE S.R.: 'SAgent: a security framework for JADE'. Proc. Fifth Int. Joint Conf. on Autonomous Agents and Multiagent Systems, 2006, pp. 1116–1118

[19] VITABILE S., CONTI V., MILITELLO C., SORBELLO F.: 'An extended JADE-S based framework for developing secure multi-agent systems', *Comput. Stand. Interfaces*, 2009, **31**, pp. 913–930

[20] ISMAIL L.: 'A secure mobile agents platform', *J. Commun.*, 2008, **3**, (2), p. 12

[21] FERNANDES D.L., SABOIA V.F.S., DE CASTRO M.F., DE SOUZA J.N.: 'A secure mobile agents platform based on a peer-to-peer infrastructure'. Int. Conf. on Networking, Systems and Mobile Communications and Learning Technologies, 2006, p. 189

[22] NOVAK P., ROLLO M., HODK J., VLEK T.: 'Communication security in multi-agent systems', *LCNS Multi-Agent Syst. Appl. III*, 2003, **1067**, p. 2691

[23] CRANEFIELD S., PURVIS M.: 'Referencing objects in FIPA SL: an analysis and proposal'. Proc. Second Int. Workshop on Challenges in Open Agent Environments at AAMAS, 2003

[24] SHAKSHUKI E., LUO Z., GONG J.: 'An agent-based approach to security service', *J. Netw. Comput. Appl.*, 2005, **28**, pp. 183–208

[25] FUGKEAW S., MANPANPANICH P., JUNTAPREMJITT S.: 'Multi-application authentication based on multi-agent system', *IAENG Int. J. Comput. Sci.*, 2007, **33**, p. 6

[26] FUGKEAW S., MANPANPANICH P., JUNTAPREMJITT S.: 'Achieving DRBAC authorization in multi-trust domains with MAS architecture and PMI'. Agent Computing and Multi-Agent Systems: 10th Pacific Rim Int. Conf. on Multi-Agent Systems, 2007

[27] MARTINEZ-GARCIA C., NAVARRO-ARRIBAS G., BORRELL J., MARTIN-CAMPILLO A.: 'An access control scheme for multi-agent systems over multi-domain environments', *LCNS Adv. Soft Comput.*, 2009, **55**, pp. 401–410

[28] MOSQUEIRA-REY E., ALONSO-BETANZOS A., GUIJARRO-BERDINAS B., ALONSO-RIOS D., LAGO-PINEIRO J.: 'A snort-based agent for a JADE multi-agent intrusion detection system', *Int. J. Intell. Inf. Database Syst.*, 2009, **3**, pp. 107–121

[29] OU C.-M., OU C.R.: 'Multi-agent artificial immune systems (MAAIS) for intrusion detection: abstraction from danger theory', *LNCS Agent Multi-Agent Syst.: Technol. Appl.*, 2009, **5559**, pp. 11–19

[30] SZYMCZYK M.: 'Detecting botnets in computer networks using multi-agent technology'. Fourth Int. Conf. on Dependability of Computer Systems, 2009

[31] TWEEDALEA J., ICHALKARANJEB N., SIOUTISB C., JARVISB B., CONSOLIB A., PHILLIPS-WRENC G.: 'Innovations in multi-agent systems', *Comput. Appl.*, 2007, **30**, pp. 1089–1115

[32] PECHOUCEK M., MARIK V.: 'Industrial deployment of multi-agent technologies: review and selected case studies', *Auton. Agent Multi-Agent Syst.*, 2008, **17**, pp. 397–431

[33] ASOKAN N., JANSON P., STEINER M., WAIDNER M.: 'The state of the art in electronic payment systems', *IEEE Comput.*, 1997, **30**, pp. 28–35

[34] ROSENBERG J., REMY D.: 'Securing web services with WS-Security' (Sams Publishing, 2004)

[35] MORADIAN E., HAKANSSON A.: 'Possible attacks on XML web service', *Int. J. Comput. Sci. Netw. Sec.*, 2006, **6**, (16), pp. 154–170

[36] HARTMAN B., FLINN D.J., BEZNOSOV K., KAWAMOTO S.: 'Mastering web services security' (John Wiley & Sons, 2003)

[37] PAPAZOGLOU M.: 'Web services: principles and technology' (Pearson Education, 2008)

[38] MORADIAN E., HAKANSSON A.: 'Approach to solving security problems using meta-agents in multi-agent system'. Conf. on Agent and Multi-Agent Systems: Technologies and Applications: KES-AMSTA, 2008

[39] PEDIREDDY T., VIDAL J.M.: 'A prototype multi-agent network security system'. Second Int. Joint Conf. on Autonomous Agents and Multiagent Systems Melbourne, Australia, 2003

[40] FASLI M.: 'On agent technology for e-commerce: trust, security, and legal issues', *Knowl. Eng. Rev.*, 2007, **22**, pp. 3–35

[41] GORODETSKI V., KOTENKO I.: 'The multi-agent systems for computer network security assurance: frameworks and case studies'. IEEE Int. Conf. on Artificial Intelligence Systems, ICAIS, 2002

[42] CHELBERG D., WELCH L., LAKSHMIKUMAR A., GILLEN M.: 'Meta-reasoning for a distributed agent architecture'. South-Eastern Symp. on System Theory Athens, Ohio, 2001

[43] MCKNIGHT D., CHOUDHURY V., KACMAR C.: 'The impact of initial customer trust on intentions to transact with a web site: a trust building model', *J. Strateg. Inf. Syst.*, 2002, **11**, pp. 297–323

[44] ZHAO S., LIU H., SUN Z.: 'Scalable trust in multi-agent e-commerce system'. Int. Symp. on Electronic Commerce and Security, 2008

[45] KARYGIANNIS A., ANTONAKAKIS E.: 'Security and privacy issues in agent-based location-aware mobile commerce', *Saf. Sec. Multi-agent Syst.*, 2009, **4324/2009**, pp. 308–329

[46] ALAGAR V.S., HOLLIDAY J., THIYAGARAJAN P.V., ZHOU B.: 'An architecture for multi-agent e-commerce transactions', http://users.encs.concordia.ca/~alagar/publications.html, last accessed 2010

[47] ZHANG D., SIMOFI S., ACIAR S., DEBENHAM J.: 'A multi agent recommender system that utilises consumer reviews in its recommendations', *Int. J. Intell. Inf. Database Syst.*, 2008, **2**, (1), pp. 69–81

[48] WEI Y.Z., JENNINGS N.R., MOREAU L., HALL W.: 'User evaluation of a market-based recommender system', *Auton. Agents Multi-agent Syst.*, 2008, **17**, pp. 251–269

[49] MARTIN A., LAKSHMI T.M., MADHUSUDANAN J.: 'Multi agent communication system for online auction with decision




doi: 10.1049/iet-ifs.2010.0041

support system by jade and trace', *J. Converg. Inf. Technol.*, 2009, **4**, pp. 154–163

[50] SHI W., JANG I., YOO H.S.: 'An efficient electronic marketplace bidding auction protocol with bid privacy', *Prog. WWW Res. Dev.*, 2008, **4978**, pp. 297–308

[51] MARQUES P., SILVA L., SILVA J.: 'Security mechanisms for using mobile agents in electronic commerce'. 18th IEEE Symp. on Reliable Distributed Systems, Lausanne, Switzerland, 1999

[52] BERGENTI F., POGGI A.: 'Multi-agent systems for e-health: recent projects and initiatives'. 10th Int. Workshop on Objects and Agents, 2009

[53] BRESCIANI P., GIORGINI P., MOURATIDIS H.: 'On security requirements analysis for multi-agent systems'. Second Int. Workshop on Software Engineering for Large-Scale Multi-Agent Systems, SELMAS Portland, Oregon, 2003

[54] ALDEA A., LOPEZ B., MORENO A., RIANO D., VALLS A.: 'A multi-agent systems for organ transplant co-ordination'. Eighth Conf. on AI in Medicine in Europe: Artificial Intelligence Medicine, 2001

[55] LI W., HOANG D.: 'A new security scheme for e-health system'. Int. Symp. Collaborative Technologies and Systems Maryland, VA, 2009

[56] SU C.J.: 'Mobile multi-agent based, distributed information platform (MADIP) for wide-area e-health monitoring', *Comput. Ind.*, 2008, **59**, (1), pp. 55–68

[57] GOKCE B., LALECI D.A., OLDUZ M., TASYURT I., YUKSEL M., OKCAN A.: 'SAPHIRE: a multi-agent system for remote healthcare monitoring through computerized clinical guidelines', in SERIES W. (ED.): 'Agent technology and e-health' (2008), Agent Technology and e-Health Whilestan Series in Software Agent Technologies, Springer and Autonomic Computing, pp. 25–44

[58] SULAIMAN R., SHARMA D., MA W., TRAN D.: 'A multi-agent security framework for e-health services', *LNCS Knowl. Based Intell. Inf. Eng. Syst.*, 2009, **4693**, pp. 547–554

[59] XIAO L., PEET A., LEWIS P., *ET AL.*: 'An adaptive security model for multi-agent systems and application to a clinical trials environment'. 31st IEEE Annual Int. Computer Software and Applications Conf. (COMPSAC'07), 2007

[60] SIERHUIS M., CLANCEY W.J., VAN HOOF R.J.J., *ET AL.*: 'Nasas OCA mirroring system. An application of multiagent systems in mission control'. Eighth Int. Conf. on Autonomous Agents and Multiagent Systems (AAMAS), 2009

[61] CHEN B., CHENG H.H., PALEN J.: 'Integrating mobile agent technology with multi-agent systems for distributed traffic detection and management systems', *Transp. Res. C*, 2009, **17**, pp. 1–10

[62] PATRICIO M.A., CARBO J., PEREZ O., GARCIA J., MOLINA J.M.: 'Multi-agent framework in visual sensor networks', *EURASIP J. Adv. Signal Process.*, 2007, **2007**, (1), p. 21

[63] JAMES G., COHEN D., DODIER R., PLATT G., PALMER D.: 'A deployed multi-agent framework for distributed energy applications'. Fifth Int. Joint Conf. on Autonomous Agents and Multiagent Systems, 2006

[64] VAUGHAN R., WISE J., HUEY P., *ET AL.*: 'Distributed multi-layered network management for NEC using multi-agent systems', *LNCS Agents Peer-to-Peer Comput.*, 2008, **4461**, pp. 159–166

[65] DAS R., KEPHART J.O., LEFURGY C., TESAURO G., LEVINE D.W., CHAN H.: 'Autonomic multi-agent management of power and performance in data centers'. Seventh Int. Joint Conf. on Autonomous Agents and Multiagent Systems: Industrial Track, 2008

[66] WANG D.G., LI T., LIU S.J., LIANG G., ZHAO K.: 'An immune multi-agent system for network intrusion detection', *Adv. Comput. Intell.*, 2008, **5370**, pp. 436–445

[67] HOLLOWAY E.M., LAMONT G.B.: 'Self organized multi-agent entangled hierarchies for network security'. Eleventh Annual Conf. Companion on Genetic and Evolutionary Computation Conf., 2009

[68] BEAUTEMEN P., ALLSOPP D., GREAVES M., *ET AL.*: 'Autonomous agents and multi-agent systems (AAMAS) for the military: Issues and challenges', *LNCS Defence Appl. Multi-Agent Syst.*, 2006, **3890/2006**, pp. 1–13

[69] CILA I., MALAB M.: 'A multi-agent architecture for modelling and simulation of small military unit combat in asymmetric warfare', *Expert Syst. Appl.*, 2010, **37**, pp. 1331–1343

[70] MANZOOR U., NEFTI S., HASAN H., MEHMOOD M., ASLAM B., SHAUKAT O.: 'A multi-agent model for mine detection – MAMMD', in 'LNCS emerging technologies and information systems for the knowledge society', Lecture notes in Computer Science, 2008, **5288/2008**, pp. 139–148

[71] BURNETT C., MASATO D., MCCALLUM M., *ET AL.*: 'Agent support for mission planning under policy constraints'. Second Annual Conf. Int. Technology Alliance, London, 2008

[72] CARLEY K.M.: 'Biodefense through city level multi-agent modelling of bio and chemical threats'. Biosurveillance Workshop, 2006

[73] XU Z., XIONG Y., REN H.: 'On agent-based strategic architecture of military medical service command system', *Appl. Softw.*, 2008, **25**, pp. 90–92