Journal of Network and Information Security
7 (2), December 2019, 09-17
http://www.publishingindia.com/jnis

Network Security Implemented With Intelligent Agent Through Multi-Agent System

Meena Sachdeva[1*] and Avadhesh Kumar[2]
[1]Uttrakhand Technical University, Dehradun, Uttarakhand, India. Email: meena@galgotiacollege.edu
[2]Galgotia University, Greater Noida, Uttar Pradesh, India. Email: Dr.avadhesh@galgotiauniversity.edu
*Corresponding Author

Abstract: Security is the process of maintaining an acceptable level of perceived risk. Nowadays, security management has become an important issue that must be considered carefully. Security is required in any organization/institute to protect its hardware, software and data resources against known or sometimes unknown resources [1]. These unknown resources cause risk to our system. Unknown resources can be inserted into system intentionally or unintentionally. We focus on one critical security management issue that is intrusion detection. So, we propose an approach for security management using intelligent agent model [2]. This model provides a flexible integration of multi-agent technique in a classical network to enhance its protection level against inherent attacks. A multi-agents system, which aims at detecting intrusions in a complex network. Multi-agents systems provide a suitable solution. So, we applied a well-known multi-agent methodology and showed that it is useful for real-life application [2]. We also used agent knowledge, with BDI theoretical model.

Keywords: Distributed network management, Intelligent agents, Intrusion detection, Multi-agent system, Network security management.

I. Introduction

Network security monitoring is defined as the collection, analysis and escalation of indications and warnings to detect and respond to intrusions. The security process revolves around four steps: assessment, protection, detection and response.

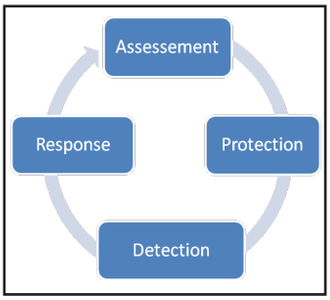

Fig. 1: Security Process

Four security steps are shown by Fig. 1.

Risk is measure of danger to an asset. Threat is a process of capability and intention of exploitation. Vulnerabilities are introduced into assets via poor design, implementation or containment. Asset value can be defined as measurement of the time and resources needed to replace an asset or restore it to its former state.

The risk equation is risk = threat × vulnerability × asset value

Intrusion is gaining unauthorized access/access exceeding one's privileges to computing resources directly or through any victim. Any successful attempt exploiting misconfiguration in system or application software, protocol, data or service is an attack. It can lead to the slowdown of system, application non-functioning, and denial of service (DoS) or system crash. Attacks can be launched from insiders (LAN users) or outsiders (from internet). Attacks can be launched on servers, networking equipment, hosts and applications [3]. Security, therefore, is not only constrained to hosts or networks but it may be extended to almost any hardware or software involved in communication till the destination is reached. The same security applies to destination system also. Intrusion-detection systems may be used to provide the required security at host or network or application level apart from encryption of information at various layers.

II. Hierarchy of Security

Fig. 2 shows how the field of security protects the general assets like hardware, software and information resources and its various subfields. There are three modes of security and applied to any circumstances. We have three D's of security and these are:

- Defense
- Deterrence
- Detection

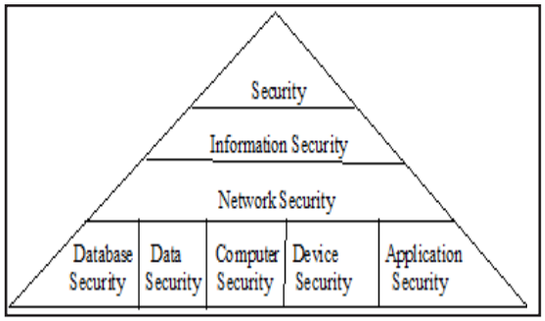

Fig. 2: Hierarchy of Security

III. Levels of Security

Different security threats are in different environments. Security threats can be boarded by different levels of security:

D -- Minimal Protection

C1 -- Discretionary Security Protection

C2 -- Controlled Access Protection

B1 -- Labeled Security Protection

B2 -- Structured Protection

B3 -- Security Domains

A1 -- Verified Design

IV. Security Mechanisms

There are two security mechanisms to increase the security. These are:

- Specific Security Mechanisms
- Pervasive Security Mechanisms

A. Specific Security Mechanisms

It handles

- Encipherment
- Digital Signature
- Access Control
- Data Integrity
- Authentication Exchange
- Traffic Padding
- Routing Control
- Notarization

B. Pervasive Security Mechanisms

It handles trusted functionality for event detection, security audit trail and security recovery.

V. Challenges of Security

Attacks challenged the security of systems, information, resources, policies, configuration, etc. Various types of security attacks, vulnerability types are as follows:

- *Security Attacks:* Security attacks are classified as:
  - Passive Attacks: Passive attacks attempts make use of information from the system but do not affect system resources.
  - Active Attacks: In active attack, hacker attempts to make changes to data.
- *Vulnerabilities Types:* Vulnerabilities can be due to software, hardware, configuration, policy, usage. Most common vulnerabilities are:
  - SQL Injections
  - Cross Site Scripting (XSS)
  - Broken Authentication & Session Management
  - Insecure Direct Object References
  - Security Misconfiguration
  - Cross-Site Request Forgery (CSRF)

VI. Attacks

Traditionally attacks on computers have included methods such as viruses, worms, buffer-overflow exploits and DoS attacks. Network attacks, on the other hand, are mostly attacks on computers that use a network in some way. A network could be used to send the attack (such as worm), or it could be the means of attack (such as Distributed Denial).

In the most widely used open source network intrusion prevention and detection system, namely the Snort, attack classification is based on its impact on the computer system [5]. The attacks whose effect is most critical have the highest priority. The priority levels are divided into high, medium and low ones. High-level priority attacks are the attempted administrator privilege gain, the network "Trojan", or the web application attack. Medium priority attacks are the DoS attacks, a nonstandard protocol or event, potentially bad traffic, attempted log-in using a suspicious user, etc. Low-level priority attacks are the ICMP event, the network scan, the generic protocol command, etc.

Computer and network attacks have evolved greatly over the last few decades [3]. The attacks are increasing in number and also improving in their strength and sophistication. Some of the trends in the history of attacks. For example: The Morris Worm, the first viruses, were released in 1981, among them Apple Viruses 1, 2 and 3 which targeted the Apple II operating system. In 1983, Fred Cohen was the first person to formally introduce the term "computer virus" in his thesis which was published in 1985.

More recently, new attacks such as DoS (mid 1990s), distributed DoS (DDoS) attacks (in 1999), botnets and storm botnets have been developed. Two recent major developments in computer and network attacks are blended attacks and information warfare. The blended attacks first appeared in 2001 with the release of Code Red and then followed by Nimda, Slammer and Blaster. Blended attacks contain two or more attacks merged together to produce a more potent attack.

A. Attack Objectives and Motivations

Attack motivation can be understood by identifying what the attackers do and how they can be classified. A simple classification of attackers is as hackers, criminals (spies, terrorists, corporate raiders and professional criminals) and vandals. The main motivation of a hacker is to access to a system or data; the main motivation of the criminal is financial or political gain; and the main motivation of the vandal is to damage [6]. In the thesis work of Howard, the problem with classifying attackers into the three categories is highlighted with all the three categories describing criminal behavior. The incidents of cyberattacks that were serious and harmful in nature can be seen to be motivated by political and social reasons as pointed out by Denning.

The potential threat of cyber terrorism becoming unavoidable is due to the critical infrastructures that are potentially vulnerable and studies show that the vulnerabilities were steadily increasing, whereas the costs of attack were decreasing [7]. The statistics of attacks in the recent years appear in the website for Web Server Intrusion Statistics.

There are various classifications of Internet attacks. These can be:

- By the goal of the attacker to
- By the effect on system like
- By the operating system on the target host
- By the attacked service

B. Commonly Encountered Attacks

Following discussion gives an extensive view of the commonly encountered attacks.

Viruses: Viruses can be defined as self-replicating programs that infect and propagate through files. Usually, they will attach themselves to a file, which will cause them to be run when the file is opened.

There are several main types of viruses as identified below:

- *File Infectors:* File infector viruses infect files on the victim's computer by inserting themselves into a file. Usually, the file is an executable file, such as an .EXE or .COM in Windows [7]. When the infected file is run, the virus executes as well.
- *System and Boot Record Infectors:* These were the most common type of virus until the mid-1990s. These types of viruses infect system areas of a computer such as the Master Boot Record (MBR) on hard disks and the DOS boot record on floppy disks. By installing itself into boot records, the virus can run itself every time the computer is booted up.
- *Macro Viruses:* Macro viruses are simply macros for popular programs, such as Microsoft Word, which are malicious. For example, they may delete information from a document or insert phrases into it. Propagation is usually through the infected files. If a user opens a document that is infected, the virus is a program that may install itself so that any subsequent documents are also infected [8]. Often, the macro virus will be attached as an apparently benign file to fool the user into infecting themselves. The Melissa virus is the example of macro virus. The virus worked by emailing a victim with an email that appeared to come from an acquaintance. The email contained a Microsoft Word document as an attachment, which if opened, would infect Microsoft Word and if the victim used the Microsoft Outlook 97 or 98 email client, the virus would be forwarded to the first 50 contacts in the victims address book. Melissa caused a significant amount of damage, as the email sent by the virus flooded email servers.

C. General Properties of Virus

Viruses often have additional properties, beyond being an infector or macro virus. A virus may also be multi-partite, stealth, encrypted or polymorphic [9]. Multi-partite viruses are hybrid viruses that infect files and system and/or boot-records. This means multi-partite viruses have the potential to be more damaging and resistant. A stealth virus is one that attempts to hide its presence. This may involve attaching itself to files that are not usually seen by the user. Viruses can use encryption to hide their payload. It is difficult to detect and analyze when he bulk of the virus is encrypted. Some viruses have the ability to change themselves as either time goes by or when they replicate themselves. Such viruses are called polymorphic viruses.

- *Worms:* A worm is a self-replicating program that propagates over a network in some way. Worms do not require an infected file to propagate. There are two main types of worms: mass-mailing worms and network-aware worms.
- *Mass-Mailing Worms:* A mass-mailing worm is a worm that spreads through email. Once the email has reached its target, it may have a payload in the form of a virus or Trojan.
- *Network-Aware Worms:* Network-aware worms generally follow a four-stage propagation model. The first step is target selection. The compromised hosts target a host.

The compromised host then attempts to gain access to the target host by exploitation. Once the worm has access to the target host, it can infect it [10]. Infection may include loading Trojans onto the target host, creating back doors or modifying files. Once infection is complete, the target host is now compromised and can be used by the worm to continue propagation. Examples are Blaster, SQL Slammer, etc.

- *Trojans:* Trojans appear to be benign programs to the user, but will actually have some malicious purpose. Trojans usually carry some payload such as remote access methods, viruses and data destruction. Trojans provide a back door for the malicious attacker and give them the following abilities: Session logging, Keystroke logging, File transfer, Program installation, Remote rebooting, Registry editing, and Process management.
- *Logic Bombs:* Logic bombs are a special form of Trojans that only release their payload once a certain condition is met. If the condition is not met, the logic bomb behaves as the program it is attempting to simulate.

VII. Analyzing Network Security

Main types of security are for password security, password sniffing, network services, protecting against attacks, access control with TCP Wrappers, Pidentd Authentication Server and port scanning.

A. Network Security Technologies

i) Cryptology: It is the science of hiding information which includes number theory, group theory, combinatory logic, complexity theory and information theory.

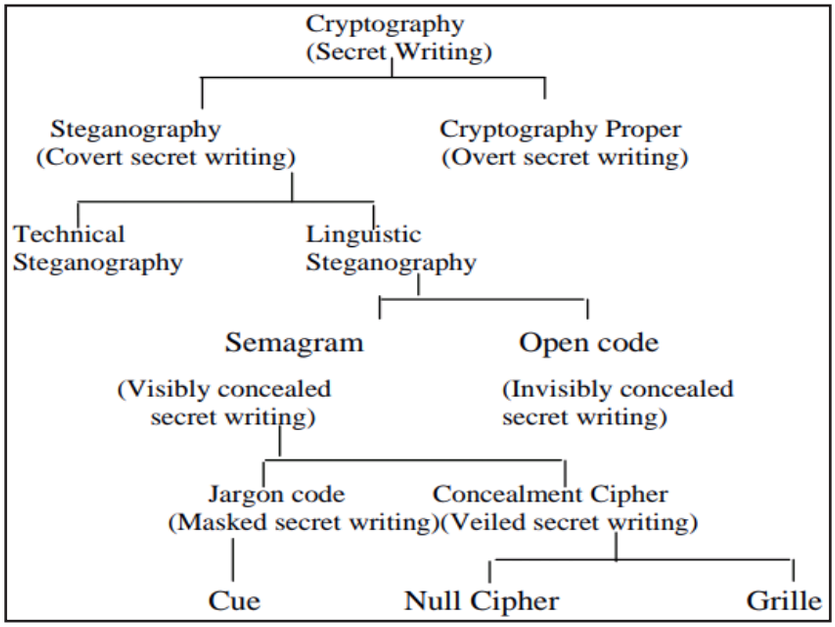

Fig. 3: Classification of Cryptography

ii) *Cryptography*: It is the art of secret writing. Fig. 3 shows the classification of cryptography.

iii) *Cryptanalysis:* Cryptanalysis is nurtured to a good part by encryption errors. It is done by:

- Exhausting Combinational Complexity
- Autonomy of language: Patterns, frequencies
- Polyalphabatic Case: Probable Words
- Compromises
- Linear Basic Analysis

iv) *Encryption:* Data can be encrypted using various encryption methods:

- Polyalphabatic Encryptions: Keys, Families of alphabets
- Composition of classes of methods
- Super encryption
- Confusion Diffusion
- Secret key cryptography---- DES, IDEA, AES
- Open encryption key systems
- Symmetric and Asymmetric Encryption Methods
- Hash Algorithms
- One way functions
- Diffie-Hellman

- RSA Method
- Digital Signature Standard (DSS)

v) Encryption Security: It is basically about framing the rules that are intended to make unauthorized decryption more difficult and is based on:

- Cryptographic Faults
- Maxims of Cryptology
- Shannon's Yardsticks

vi) Steganography: It is art of secret writing. It is of following types:

- Watermarking and fingerprinting
- Steganography in Media
- Steganography Text
- Steganography Images
- Steganography Audio

VIII. The Agent Model

To model intrusion detection, agents must combine cognitive abilities (knowledge-based) to reason about complex attacks with reactive capacities (stimulus-response) to react rapidly to the environments changes [11]. So, an agent has three functions: 1) a filtering function that filters security events, 2) an interaction function that manages its interactions with environment and other agents, and 3) a deliberation function that enables it to analyze new data and detect attacks. These functions are described in Fig. 4.

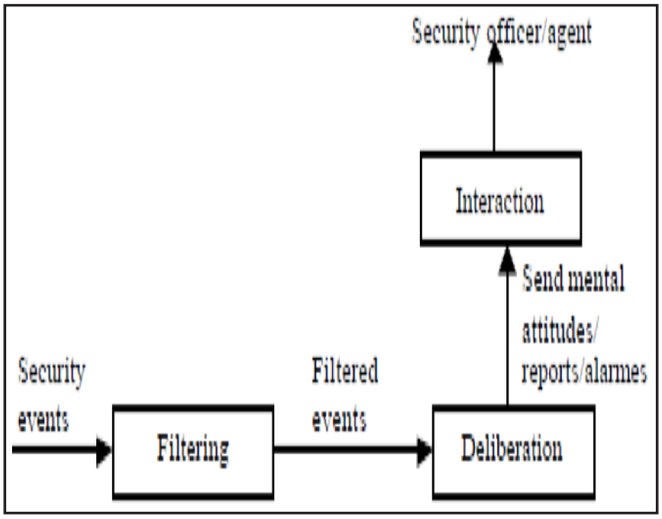

Fig. 4: Agent Model

IX. Event Filtering Function

A security event is characterized by its type, its observation point, a temporal attribute (representing the event occurring moment), and a set of non-temporal attributes. According to the event type and its observation point, we identify various event classes by Fig. 5.

The event filtering function filters security events produced in the network, according to event classes specified in a detection goal. Indeed, the events occurring in network are not all collected. In fact, when a detection goal is sent to an agent, a set of event classes to observe is specified to it. Thus, when an event occurs in the network, the agent tests if it matches the event classes specified in the goal [12]. If it matches, it is collected. The filtered events are then stored, waiting to be treated by the deliberation function.

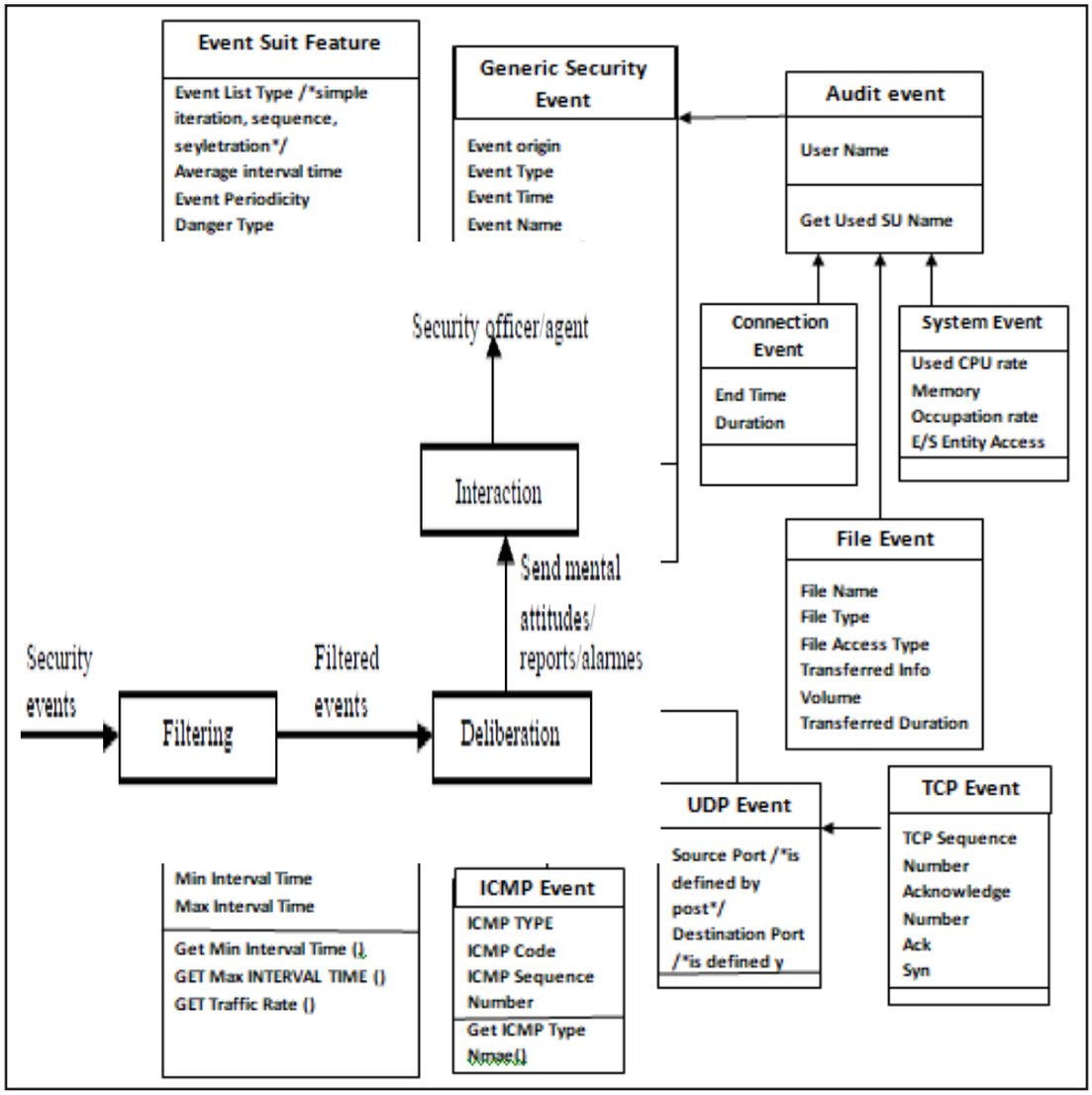

Fig. 5: Event Filtering Function

A. Interaction Function

This function describes interactions between the above-described agents. It allows them to communicate their analyses and knowledge and mental attitudes (beliefs, suspicions…). In fact, manager agents interact with local agents by: sending goals, derived from security policies; delegating specific functions of monitoring/detection and specifying the various domains to monitor; asking particular information: the suspicion level of a specific user, the list of events generated by a user, etc.; and receiving the relevant reports or analyses results and alarms [13]. Interaction function also permits interactions between the security officer and security policy manager agent/extranet manager agent. It ensures the reception of specifications and requests from the security officer such as security policies to apply. It allows the delivery of security reports and alarms when an attack is detected [16]. The security officer can also ask for additional information.

B. Deliberation Function

Security management must deal with significant network characteristics such as: 1) its continuous variation, particularly in terms of users and offered services; 2) and variation of its security problems such as new vulnerabilities and increasingly complex attacks. Considering the unpredictable character of the agent environment behavior (network), we adopted a BDI solution for modelling the security management system [14]. Thanks to the deliberation function the agent. In this section,

we will start by describing the knowledge base of the agent and then the BDI-based information model.

i) Knowledge Base: The knowledge base of the agent contains two types of knowledge:

- *Immediate Character Knowledge* that represents the observations made by the agent (events produced in the network) on its environment [15]. This knowledge has a limited validity lifetime·
- *Permanent Character Knowledge,* which represents the necessary knowledge for managing security of the network (such as list of known user/user groups, list of administrators, list of known hosts, list of known addresses, prohibited addresses, reserved addresses).

ii) BDI-Based Information Model: This model represents the mental attitudes of the security agent: beliefs, goals, intentions, suspicions and policies.

- *Beliefs:* Beliefs represent the perception that the agent has on the network behavior and its security state.
- *Goals:* Goals represent the state that must be reached by the agent viz. its objectives.
- *Intentions:* Intentions represent the list of actions that must be executed by the agent when it achieves its goal. These actions can be sending alarms to the security officer or manager agent, closing a connection established by an attacker, and reconfiguring a firewall.
- *Suspicions:* This mental attitude, introduced within the framework of intrusion detection, expresses the suspicion that has an agent on a scenario belief. When an agent observes a sequence of events which corresponds neither to a normal sequence, nor to a known attack, then it identifies it as suspicious sequence [19]. To confirm that this suspicion is an attack, the agent needs further information or confirmations from other agents. The agent will then say to other agents: "I suspect that this sequence of events is an attack". A suspicion is associated to a schema belief and is the result of the analysis of a scenario belief compared to a schema belief.
- *Policies:* Policies represent the guiding mental attitude of the MAS behavior to manage the security of the company. Starting from the specified security policies, a set of *goals* are created and derived in order to maintain a certain security state of the network.

X. Implementation

The presented agent model has been implemented with the multi-agent platform DIMA architecture. DIMA proposes the extension of the single behavior of an active object into a set of behaviors. In our implementation, each agent has the following three behaviors [18]:

The filtering behavior filters security events. When an event occurs in the network, it is collected only if it matches the event classes specified in the detection goal.

EventFilter {

Repeat

security-event: = get(security-event-to-filter);

If is-in-list-of-event-types-to-filter(security-event)

Update-list-of-filtered-event(security-event);

end repeat }

The interaction behavior manages the interaction between the agent and the other agents [17]. It defines the mailbox of the agent and the way the messages are received and enquired for later interpretation. An agent may need some others information to refine its analysis [20]. In this case, it asks other agents to give it the necessary information.

The *deliberation* behavior represents beliefs, goals, intentions and knowledge of the agent. It is responsible 1) for generating adequate responses to the messages received from the other agents and 2) for achieving the agent goal(s).

When an agent receives a *detection goal*, it updates a set of event classes to filter. Then, when an event occurs, it is filtered by the filtering module and sent to the deliberation module. This one updates/creates agent scenario beliefs and then test if this is about belief. If it matches, then a detection goal is reached and a list of intentions is sent to the interaction module for being executed.

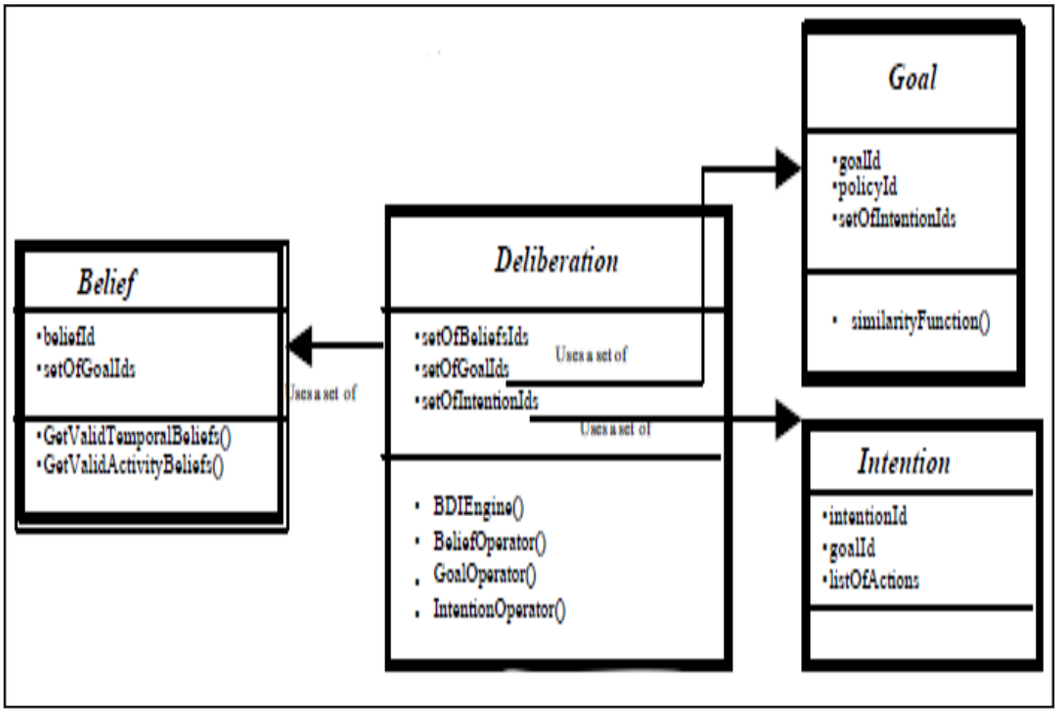

Fig. 6: UML Classes

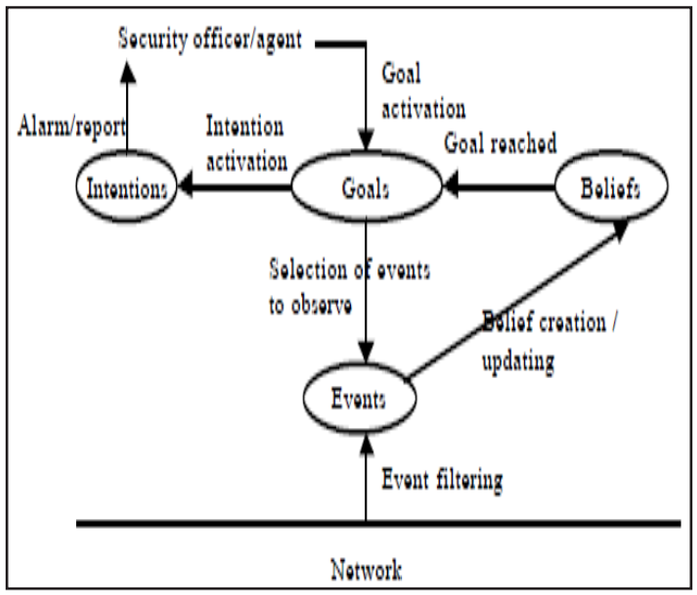

Fig. 7: Interaction between Mental Attitudes

References

[1] K. Boudaoud, H. Labiod, R. Boutaba, and Z. Guessoum, "Network security management with intelligent agents," *NOMS 2000. 2000 IEEE/IFIP Network Operations and Management Symposium 'The Networked Planet: Management Beyond 2000' (Cat. No. 00CB37074)*, Honolulu, USA, Apr. 10-14, 2000.

[2] K. Boudaoud, and Z. Guessoum, "A multi-agents system for network security management," *Telecommunication Network Intelligence, IFIP TC6 WG6.7 Sixth Int. Conf. on Intelligence in Networks (SMARTNET 2000*), Vienna, Austria, Sept. 18-22, 2000.

[3] H. K. Song, K. M. Kim, K. T. Kim, and H. Y. Youn, "Application of genetic algorithm for logistics based on

multi-agent system," In *2013 Int. Conf. on Information Networking (ICOIN),* vol. 1, pp. 309-314, IEEE, 2013.

[4] S. Bijani, and D. Robertson, "A review of attacks and security approaches in open multi-agent systems," *Artificial Intelligence Review*, pp. 1-30, Springer, May, 2012.

[5] W. Ho, H. Higson, P. K. Dey, X. Xu, and R. Bahsoon, "Measuring performance of virtual learning environment system in higher education," *Quality Assurance in Education*, vol. 17, no. 1, pp. 6-29, 2009.

[6] R. H. Bordini, A. E. F. Seghrouchni, and M. Dastani, *Multi-Agent Programming: Languages, Platforms and Applications*, Springer, 2009.

[7] T. Erl, A. Karmarkar, P. Walmsley, H. Haas, ... and J. Pasley, *Web Service Contract Design and Versioning for SOA*, Prentice Hall, 2009.

[8] "E-business systems," *International Journal of Business and Information*, vol. 3, no. 1, pp. 129-143, 2008.

[9] E. M. van Raaij, and J. J. L. Schepers, "The acceptance and use of a virtual learning environment in China," *Computers & Education*, vol. 50, no. 3, pp. 838-852, 2008.

[10] A. Kannammal, and N. Iyengar, "A framework for mobile agent security in distributed agent based e-business systems," *International Journal of Business and Information*, vol. 3, no. 1, pp. 129-143, 2008.

[11] S. D. Ramchurn, D. Huynh, and N. R. Jennings, "Trust in multi-agent systems," *The Knowledge Engineering Review*, vol. 19, no. 1, pp. 1-25, 2004.

[12] M.-H. Lin, C.-C. Chang, and Y.-R. Chen, "A fair and secure mobile agent environment based on blind signature and proxy host," *Computers & Security*, vol. 23, no. 3, pp. 199-212, 2004.

[13] D. Tavangarian, M. E. Leypold, K. Nölting, M. Röser, and D. Voigt, "Is e-learning the solution for individual learning," *Electronic Journal of e-Learning*, vol. 2, no. 2, pp. 273-280, 2004.

[14] Z. Guessoum, and J.-P. Briot. "From active object to autonomous agents," *IEEE Concurrency,* vol. 7, no. 3, pp. 68-78, July/September, 1999.

[15] R. F. Teixeira, and D. Oliveira, "Gestion des réseaux avec connaissance des besoins: Utilisation des agents logiciel," PhD Thesis, Eurécom Institute, France, 1998.

[16] S. Corley, and et al., "The application of intelligent agent technologies to network and service management," *5th IS&N Conf.*, Antwerpen, Belgium, May 25-28, 1998.

[17] J. Ferber, and O. Gutknecht, "A meta-model for the analysis and design of organizations in multi-agent systems," ICMAS, 1998.

[18] G. B. White, E. A. Fisch, and U. W. Pooch, "Cooperating security managers: A peer-based intrusion detection system," *IEEE Network*, vol. 10, no. 1, pp. 20-23, January/February, 1996.

[19] J. Ferber, *Les Systèmes Multi-Agents, Vers Une Intelligence Collective*, InterEd. 1995.

[20] A. Rao, and M. Georgeff, "BDI Agents: From Theory to Practice," Tech. Note 56, 1995.

[21] M. Wooldridge, and N. R. Jennings, "Intelligent agents: Theory and practice," *Knowledge Engineering Review*, vol. 10, no. 2, pp. 115-152, 1995.