INTERNATIONAL RESEARCH JOURNAL IN ADVANCED ENGINEERING AND TECHNOLOGY (IRJAET) E - ISSN: 2454-4752 P - ISSN : 2454-4744
VOL 2 ISSUE 3 (2016) PAGES 989-992
RECEIVED : 01/05/2016. PUBLISHED : 24/05/2016
May 24, 2016

GROUP MODELLING OF SECURITY ALERT AND ANALYSIS FOR INTRUDER DETECTION IN ROBOTIC NETWORK

[1]Karthikeyan.S, [2]Madhan.N, [3]Muthuselvi.G, [4]Sudhakaran.M,
[1,2]Student, Dept of EEE, GTEC Engineering college, vellore,
[3]Asst prof, Dept of EEE, GTEC Engineering college, vellore.
[4]Asso prof, Dept of EEE, GTEC Engineering college, vellore.

Abstract:
Multi-agent systems are currently applied to solve complex problems. The security of networks is an eloquent example of a complex and difficult problem. A new model-concept Hybrid Sensitive Robot Metaheuristic for Intrusion Detection is introduced in the current paper. The proposed technique could be used with machine learning based intrusion detection techniques. The new model uses the reaction of virtual sensitive robots to different stigmergic variables in order to keep the tracks of the intruders when securing a sensor network.

Keywords: intrusion detection, sensor network, intelligent agents.

1. INTRODUCTION

Prevention and detection of intruders in a secure net- work is nowadays a challenging issue. The intrusion detec- tion system based on computational intelligence (CI) has proved in time to have huge advantages over traditional detection systems due to characteristics of CI methods: adaptation, fault tolerance, high computational speed etc. It is essential to design efficient Intrusion Detection Sys- tems (IDS) especially for open medium networks as wire- less sensor devices. The intrusions could be missue intrusions and anomaly intrusions. Missue intrusions are the attacks knowing the weak points of a system. Anomaly intrusions are based on observations of normal system usage patterns and de- tecting deviations from the given norm. The mentioned intrusions are hard to quantify because there are no fixed patterns that can be monitored and as a result a more fuzzy approach is often required. The Intrusion Preventing Systems (IPS) are network security appliances that monitor network and/or system activities for malicious activities. IPS is a device used to block all the unwanted access to the targeted host, to remove malicious part of packets and as well it may re- configure the network device where an attack is detected [3]. The aim of the current paper is to provide an effective stigmergic-based technique for IDS in a sensor network graph, that consist of multiple detection stations called sensor nodes. The new Hybrid Sensitive Robot Metaheuris- tic for Intrusion Detection (HSRM-ID) model uses a col- lection of robots endowed with a stigmergic sensitivity level. The sensitivity of robots allow them to detect and react to different stigmergic variables involving the attacks into a secure network. The hybrid model combines ele- ments from Sensitive Robot Metaheuristic (SRM) [19] as Ant Colony System (ACS) [10], autonomous mobile robots and the intrusion detection based on emotional ants for sensors (IDEAS).

2. STRICMERGIC ROBOTS

The metaheuristic Sensitive Robot Metaheuristic combining the concepts of stigmergic communication and autonomous robot search is used to solve NP-hard optimization problems. An

important characteristic of stigmery is that indi- vidual behavior modifies the environment, which in turn modifies the behavior of other individuals [11]. The SRM technique attempts to address the coupling between per- ception and action as direct as possible in an intelligent stigmergic manner. As it is known, robot communication relies on local en- vironmental modifications that can trigger specific actions. The set of the rules defining actions (stimuli pairs) used by a homogeneous group of stigmergic robots defines their be- havior and determines the type of structure the robots will create . Robot stigmergic communication does not rely on chemical deposition as it is for artificial ant-based colonies [10]. A stigmergic robot action is determined by the environmental modifications caused by prior actions of other robots. The value of quantitative stigmergy modify the future actions of robots. Discrete stimulus are involved in qualitative stigmergy and the action is switched to a dif- ferent action [4, 26]. Some real-life applications of the behavior-based ap- proach, including autonomous robots, are in data min- ing, military applications, industry and agriculture, waste management, health care. Lee et al. [15] introduced a data mining classification mechanism with association rules from the audit data - knowledge present in a knowledge base - providing gaudi- ness for data gathering and feature selection. In order to detect abnormal behavior one can use genetic algorithms, see for example [1]. In [18], neural networks use back prop- agation MLP for a small network in order to detect anoma- lies and identify user profiles after end of each log session. The proposed (HSRM) can be modelled using two dis- tinct groups of sensitive stigmergic robots. The first group of robots-agentsis endowed with small sensitive values SSL and they are sensitive-explorers (sSSL: small SSL-robots). They can sustain diversification in intruders searching. In the second group are the robots-agents with high sensi- tive stigmergic values (hSSL: high SSL-robots).

3. NEW CONCEPT

In the following is performed an analyze of the Hybrid Sensitive Robot Algorithm for Intrusion Detection. The artificial pheromone from the edges of the sensor network graph reveals as the attacked zone within the network. Each bio-inspired robot uses his one specific properties as his level of sensitivity in order to detect the intruders and the artificial stigmergy in order to find the attacked edges. Table 1 illustrates the behavior of different groups of sensi- tive bio-inspired virtual robots when investigate the sensor network in search of intrusion. As a concept, the intro- duced model Hybrid Sensitive Robot Algorithm for Intru- sion Detection has more chances to improve the intrusion detection systems comparing with the existing approaches from the literature, due to the sensitivity property of the bio-inspired robots. As well the diversity of robots groups implies also different values of virtual pheromone trail val- ues. The robots with small stigmergic value are constantly sustaining diversification in intruders searching and as a complementary action, the robots with high sensitive stig- mergic values are testing the already identified networks attacked regions. In the future we will perform numeri- cal experiments to assess the performance of the proposed algorithm.

4. INTRUSION DETECTION TECHNIQUES USING ARTIFCIAL INTELLIGENCE

At first are introduced the main concepts of IDS followed by a survey of Artificial Intelligence-based existing models for computer security. ntrusion detection technology is a technol- ogy designed to monitor computer activities for the purpose of finding security violations. IPS is able to detect and prevent attacks but it has not deeper detection capabilities of IDS. Neither of Intru- sion Detecting System and Intrusion Prevention System is capable to provide in depth security. Intrusion Detect- ing and Prevention System I(IDPS), a combinations of IDS and IPS, is a more effective system capable of detection and prevention. An example of network-based system is Snort [14]. Snort is an open source network intrusion prevention and detection system - nowadays a standard for IPS - that combines the

benefits of signature, protocol and anomaly-based inspection. host-based systems describe the class of software able to monitor a single system, analyse characteristics and log to at one host. These systems are deployed on critical hosts. wireless-based systems analyse wireless traffic to mon- itor intrusion or any suspicious activity. They scan traffic but are not able to identify attack in the ap- plication layer or higher layer network protocols as UDP and TCP. It may be deployed at the point where unauthorized wireless network could be ac- cessed. According to Beg et al. [3], the intrusion detection classical algorithms have the following disadvantages: false alarm rate and constant updates of database with new sig- natures. The network administrator responds to alarms and updates the signatures that increases in time. For example, in the already mentioned Snort signatures in- creased from 1500 to 2800 over two years [14]. In order to improve the administrator work, reducing the number of false alarms and better intrusion detection are intro- duced artificial intelligence mechanisms [23]. Some of AI techniques used in intrusion detection are data mining, genetic algorithm, neural network, multi-agents, ant-net miner, etc. Lee et al. [15] introduced a data mining classification mechanism with association rules from the audit data - knowledge present in a knowledge base - providing gaudi- ness for data gathering and feature selection. In order to detect abnormal behavior one can use genetic algorithms, see for example [1]. In [18], neural networks use back prop- agation MLP for a small network in order to detect anoma- lies and identify user profiles after end of each log session. It shall also be remarked that several of the leading methods for detecting intrusions and detecting intrusions are hybrid artificial approaches, which combine different AI solution techniques [9, 16, 25]. Some hybrid meth- ods used in the literature are data mining and fuzzy logic techniques [16], data mining and genetic algorithm select- ing the best rules for the system [9]. In the future could be implemented hybrid models involving intelligent evolu- tionary agents [12] and dynamic decision boundary using Support Vector Machine [24] for handle a large number of features. Banerjee et al. [2] introduced an intrusion detection based on emotional ants for sensors (IDEAS), which could keep track of the intruder trials. This technique is able to work in conjunction with the conventional machine learn- ing based intrusion detection techniques to secure the sen- sor networks.

5. HYBRID SENSITIVE ROBOT METAHEURISTIC FOR IN- TRUSION DETECTION

In this section we introduce a new hybrid metaheuristic in order to detect the intruders in a sensor network. The new model is called Hybrid Sensitive Robot Metaheuristic for Intrusion Detection (HSRM-ID), is based on Sensitive Robot Metaheuristic (SRM) introduced in [19] and uses a specific rule in order to generate a state of thinking or the choice of an intruder [2]. The proposed (HSRM) can be modelled using two dis- tinct groups of sensitive stigmergic robots. The first group of robots-agentsis endowed with small sensitive values SSL and they are sensitive-explorers (sSSL: small SSL-robots). They can sustain diversification in intruders searching. In the second group are the robots-agents with high sensi- tive stigmergic values (hSSL: high SSL-robots). They are ensitive-exploiters and could exploit intensively the re- gions already identified with attacks from intruders. In time, based on the experience of robots-agents, the sensi- tive stigmergic level SSL can increase or decrease. The pseudo-code description of the Hybrid Sensitive Robot Metaheuristic for Intrusion Detection is described in what it follows. The stigmergic value of an edge is τ and the visibility value is η. A tabu list with the already visited nodes is maintained, see [10] for more details. In order to divide the colony of m robots in two groups it is used a random variable uniformly distributed over [0,1]. Let q be a realization of this random variable and q0 a constant $0 \leq q0 \leq 1$. If the inequality $q > q0$ stands the robots are endowed with small sensitive stigmergic value sSSL robots and otherwise they are highly sensitive stig- mergic robots (hSSL). A hSSL-robot uses the information supplied by the sSSL robots.

CONCLUSION

Nowadays the networks are threatened by security at- tacks and resource limitations. In order to deal with this security network problem efficient intruders detection and prevention systems are used. Within this paper we in- troduce a new concept Hybrid Sensitive Robot Algorithm for Intrusion Detection based on bio-inspired robots. It is used a qualitative stigmergic mechanism, each robot is endowed with a stigmergic sensitivity level facilitating the exploration and exploitation of the search space. In the future some computational tests will be proposed and fur- ther hybrid AI techniques will be involved for securing the networks.

REFERENCES

[1] L. Alhazzaa. Intrusion Detection Systems using Genetic Algo- rithms. 2007.

[2] S. Banerjee, C. Grosan and A. Abraham. IDEAS: Intrusion De- tection based on Emotional Ants for Sensors. Intelligent Sys- tems Design and Applications. IEEE C.S. 344–349, 2005.

[3] S. Beg, U. Naru, M. Ashraf and S. Mohsin. Feasibility of Intru- sion Detection System with High Performance Computing: A Survey. Int. J. for Advances in Computer Science. 1(1):26–35, 2010.

[4] E. Bonabeau, M. Dorigo and G. Tehraulaz. Swarm intelligence from natural to artificial systems. Oxford, UK: Oxford Univ. Press, 1999.

[5] C. Chira, C-M. Pintea and D. Dumitrescu. Sensitive stigmergic agent systems: a hybrid approach to combinatorial optimiza- tion. Innovations in Hybrid Intelligent Systems, Advances in Soft Computing, 44:33–39, 2008.

[6] C. Chira, C-M. Pintea and D. Dumitrescu. Cooperative learning sensitive agent system for combinatorial optimization. NICSO 2007, Studies in Computational Intelligence, 129:347–355, 2008.

[7] C. Chira, D. Dumitrescu and C-M. Pintea. Learning sensitive stigmergic agents for solving complex problems. Computing and Informatics, 29(3):337–356, 2010.

[8] T. Crothers. Implementing Intrusion Detection Systems, Wiley, 2003.

[9] Y. Dhanalakshmi and I. R. Babu. Intrusion detection using data mining along fuzzy logic and genetic algorithms. Int. J. of Com- puter Science and Network Security, 8(2):27–32, 2008.

[10] M. Dorigo and L. M. Gambardella. Ant Colony System:A coop- erative learning approach to the Traveling Salesman Problem. IEEE Trans.Evol.Comp. 1:53–66, 1997.

[11] Grass´e, P.-P. La Reconstruction du Nid et Les Coordinations In- terindividuelles Chez Bellicositermes Natalensis et Cubitermes. Insect Soc. 6:41–80, 1959.

[12] B. Iantovics and C. Enachescu. Intelligent Complex Evolution- ary Agent-based Systems. Development of Intelligent and Com- plex Systems. AIP, 116-124, 2009.

[13] N. Ierace, C. Urrutia and R. Bassett. Intrusion Prevention Sys- tems. Ubiquity, ACM, 2–2, 2005.