Intrusion detection system performance in ubiquitous environments using genetic algorithm approach

Lynda SELLAMI
Department of Computer Science
Bejaia University,
ALGERIA
slynda1@yahoo.fr

The objective of ubiquitous systems is to give users the ability to communicate and provide information regardless of their location in the network.Ubiquitous computing is set of technologies (hardware and/or software) present in our daily service [8]. Ubiquitous computing allows passing from the use of a single device by a group of users toward use a group of equipment by a single user [3]. These equipment need to communicate and interact with their environment, with intention of cooperate and easy access to information. In such environment, the user will be taken into account by its physical context for the purpose of having a mobile access to data and processing, for offer the best services [1] [2].

Objective of man is have gives the possibility and capacity to communicate and to procure information and service anyway. Ubiquitous and pervasive computing is improving the lives of men (people) in making their service, and facilitates access to information at all times, assuring comfort, safety and/or assistance in the daily activities of people [6].

Advantage of ubiquitous and pervasive computing is a flexibility of devices and accessibility of service and information, these advantages exposes the network to malicious activity.

However, security is always a fundamental issue in ubiquitous and pervasive computing environment, because these networks differ from traditional networks and thus have special characteristics such as shared resources, node mobility, and availability of service and information, etc. This special characteristics necessity detect malicious activity in near real-time and raise an alert. This is the role of intrusion detection systems (IDSs).

Intrusion detection is the discovery or identification of the use of a computer system for purposes other than those intended. Intrusion detection intrusion system is a system that performs automatically the process of intrusion detection [5]. IDS allow identifying abuse of computer system, being that unauthorises extern use, direct attack on computing resources, on interne misuse.

For made the detection of intrusion, we have need to data to extract from a data source. Once this data is collected, it must be analyzed using approach (principle) detection [7]. The using the intrusion detection system to following frequency of use; A behavior to this attack is performed once an attack is eventually detected [4].

The intrusion detection systems have largely was evoked for solving the problems intrusions in networks, there are several solutions was adopted them for several situations and vulnerabilities.

To cope with vulnerabilities introduced by the computer; security and privacy guarantees in computing environments, multiple intrusion detection systems (IDS) have been implemented; the first distributed IDS that has been developed is the DIDS [8] for The distributed intrusion detection system. It consists of a central manager and multiple controllers. The central manager has access to audit data collected by distributed controllers. The central manager is responsible for analyzing and correlating events recorded. It is responsible for receiving reports of controllers and managers LAN, it treat, corrects reports, and detects the intrusions. The central manager uses an expert system for the evaluation and transmission of the status of network security.

Grids (for The Graph- based Intrusion Detection System) [10] is another distributed IDS. It is based on graphs of activity. The system is divided and observed into domains. Each domain developed its own activity graph and transmits the graph and summarizes information to its parent domain.

Cooperative IDSs have been proposed for ad hoc networks [3]. The system consists in clusters; each cluster has a controller who is elected as leader of the cluster by neighboring nodes. The detection module must be installed

on each host. It is therefore necessary to have a capacity (power) in the host to perform detection tasks. Each node participates in intrusion detection and response

Other solutions (IDS) based on mobile agents have been developed. In [9], the authors presented AAFID (for Automous Agents For Intrusion Detection) which can be distributed over multiple computers. Each host has a transceiver, a filter and a number of agents. Agents send the results to the transceiver. It communicates the results of the test (analysis) controllers. The controllers are responsible for making intrusion detection. The agents monitor user behavior stations. Controllersbuild the global state of the network.

In these solutions, several analytical techniques / metaheuristics are used. Our goal in this paper is to explore the possibility of detecting intrusions (attacks) occurred in ubiquitous environments using genetic algorithm approach.

Keywords— Ubiquitous computing; Security ;IDS; privacy; trust;

References

1 RébeccaDeneckère, Elena Kornyshova. “La variabilité dueà la sensibilité au contexte dans les processustéléologiques”. Publié dans "INFORSID, Marseille :France (2010)

2 Pierre-Yves Gicque “Mobilité et sensibilité au contexte.ICI19 - Interaction homme machine. 24 Novembre 2010

3 Y. Huang, W. Lee, “A cooperative intrusion detection system for ad-hoc networks”, in: Proceedings of the 1st ACM Workshop on Security of Ad Hoc and Sensor Networks (in association with 10th ACM Conference on Computer and Communications Security), Washington, DC, USA, 2003, pp. 131–147.

4 Julien Lancia. ”Infrastructure orientée service pour ledéveloppement d’application ubiquitaire”. Thèse.N_d’ordre : 3745. 2008.

5 LudovicMé&Cédric Michel." La détection d’intrusion :bref aperçu et derniers développements". Mars 1999

6 OECD. Guidelines on the protection of privacy andtransborder flows of personal data”, 1980.

7 Biondi Philippe: " Architecture expérimentale pour la détection d’intrusions dans un système informatique". AvrilSeptembre 2001

8 S. Snapp, J. Brentano, G. Dias, T. Goan, et al., “A system for distributed intrusion detection”, COMPCON Spring 1991, Digest of Papers, San Francisco, USA, 1991, pp. 170–176.

9 E. Spafford, D. Zamboni, “ntrusion detection using autonomous agents”, Computer Networks 34 (4). 2000.

10 S. Staniford-Chen, S. Cheung, R. Crawford, M. Dilger, J. Frank, J. Hoagland, K. Levitt, C. Wee, R. Yip, D. Zerkle, “GrIDS – a graph based intrusion detection system for large networks”, in: Proceedings of the 19th National Information Systems Security Conference, vol. 1, National Institute of Standards and Technology, Oct. 1996, pp. 361–370.