# A Mobile Agent Approach for IDS in Mobile Ad Hoc Network

.

YOUSEF EL MOURABIT, AHMED TOUMANARI, HICHAM ZOUGAGH
Laboratory Signaux system & Informatique, ENSA Agadir, IBN ZOHR University
AGADIR, MOROCCO

**Abstract:**

Mobile Ad Hoc Networks are a group of wireless computers, forming a communication network, that have no predetermined structure. It's highly vulnerable to attacks due to the open medium dynamically changing network topology,
co-operative algorithm, lack of centralized. The fact that security is a critical problem. This work describes the proposal for an Intrusion Detection System architecture that uses multi-agent system. It's an effective choice for many research and application areas due to several reasons, including improvements in latency, reducing network load and threat assessment. To respect the main primitives of a multi-agent system, we used the MadKit platform for implementation.

***Keywords***

*MANET, Multi-Agent System, IDS, MadKit, mobile agent.*

## 1. Introduction

Security in Mobile Ad-Hoc Network (MANET) is the most important concern for the basic functionality of network. Availability of network services, confidentiality and integrity of the data can be achieved by assuring that security issues have been met. MANET often suffer from security attacks because of its features like open medium, changing its topology dynamically, lack of central monitoring and management, cooperative algorithms and no clear defense mechanism.[1]

Because the Mobile Ad Hoc Network has characteristics of wireless connected signal channel, autonomous mobile node, network topology in dynamic change and weak security authentication mechanism, in addition, it is easier to suffer various security threats and attacks form passive eaves dropping to active impersonation, message playback, message falsification, and denial of service, etc. [2] Therefore, the Intrusion Detection System (IDS) comes into the second firewall of network security solution. Intrusion detection is one of the key techniques behind protecting a network against intruders. An intrusion detection system tries to detect and alert on attempted intrusions into a system or network, where an intrusion is considered to be any unauthorized or unwanted activity on that system or network. An IDS is a defense system that detects hostile activities in a network and then tries to possibly prevent such activities that may compromise system security.

The low detecting speed and high false positive rate of traditional intrusion detection system, the Intelligent and mobile characteristics of the agent are principals reasons to propose a new architecture of intrusion detection system based on mobile agent.

## 2. Related work

This section explores the work of researchers in the fields of mobile agent for intrusion detection systm and highlighted the areas of potential scope for research :

DIDMA performs decentralized data analysis using mobile agents that makes it more scalable. DIDMA uses platform independent components in contrary to platform specific security managers of CSM. The Autonomous Agents for Intrusion Detection (AAFID) project [3] makes use of multiple layers of agents organized in a hierarchical structure with

each layer performing a set of intrusion detection tasks. A proposed efficient anomaly intrusion detection system in Ad-hoc by mobile agents[4] which uses the data mining algorithm to detect the attacks exploited by the intruders. Mobile agent based intrusion detection system for MANET [5] proposed by yinan Li which uses the clustering and joint detection technique to identify the intruders.
Literature review [6,7,8,9] brought up the fact that although many attempts have been made to provide security in MASs (Mobile Agent Systems) communication and establishing trust among the agents, many rigid technologies developed to support security; but as the wheel of the technology spins every time, so the area always needs further refined researches in every approach we take.

## 3. Survey of Mobile Agent and IDS

### *3.1 Mobile Agent*

Mobile Agents are the programs that move between computers or nodes of network, autonomously trying to fulfill some specific goals given by users. Agents are different from other applications in that they are goal- oriented: they represent users and act on their behalf to achieve some set goals in an autonomous manner – i.e. they control themselves, as in the decision where and when they will move to the next computer or node. Mobile Agents do provide a viable means of performing network security assessment and analysis efficiently and effectively. Mobile agent neither brings new method to detect for IDS nor increases detection speed for some kind of attracting. Nevertheless, it improves the design, construct, and execute of IDS obviously. Mobile agents offer several potential advantages that may overcome limitations that exist in static, centralized components :

***Reducing Network Load:***

Instead of sending huge amount of data to the data processing unit, it might be simpler to move the processing algorithm (i.e. agent) to the data.

***Overcoming Network Latency:***

When agents operate directly on the host where an action has to be initiated, they can respond faster than the tree based systems that have to communicate with a central coordinator located elsewhere on the network.

***Autonomous Execution :***

When portions of the tree based systems get destroyed or separated, it is important for the other components to remain functional. Independent mobile agents can still act and do useful work when their creating platform is unreachable which increases the fault-tolerance of the overall system.

***Heterogeneous Environment:***

The agent platform allows agents to travel in a heterogeneous environment and inserts an OS independent layer.

***Dynamic Adoption:***

The mobility of the agents can be used to reconfigure the system at run-time by having special agents move to a location where an attack currently takes place to collect additional data.

***Scalability :***

when distributed mobile agents replace a central processing unit, the computational load is divided between different machines and the network load is reduced. This enhances scalability and additionally supports fault-resistant behavior [10].

### *3.2 IDS*

IDSs are hardware and software systems that monitor events occurred on computers and computer networks in order to analyze security problems. IDS and firewalls have become key components in ensuring the safety of network systems. Intrusions and invasions inside computer networks are called as “attacks” and these attacks threaten the security of networks by violating privacy, integrity and accessibility mechanisms. Attacks can be originated from users who login to the computer using Internet trying to gain administrator rights and other users who misuse the rights they have. IDSs automate monitoring and analyzing the attacks [11, 12, 13].
In general, the IDSs are composed of four components (sensors, analyzers, database and response units) and are responsible for activities such as monitoring the users and systems activities, auditing systems configuration, accessing data files, recognizing known attacks, identifying odd

activities, auditing data manipulation, tagging normal activities, error correction and storing information concerning invaders [14].
There are four basic techniques used to detect intruders:
Anomaly detection, misuse detection (signature detection), target monitoring, stealth Probes.

## 4. Proposed Work

We propose a new Intrusion detection system based on the mobile agent.which employ statistical classification algorithms to order to perform intrusion detection in MANETs. Such algorithms have the advantages that they are largely automated, that they can be quite accurate, and that they are rooted in statistics. For that reason, they are prime candidates for use in cost-sensitive classification problems. After training, they can be used for detection with arbitrary cost matrices. They have extended applications including intrusion detection in wired networks [18], they have been extensively studied, both theoretically and experimentally, and used in many applications with a high degree of success.

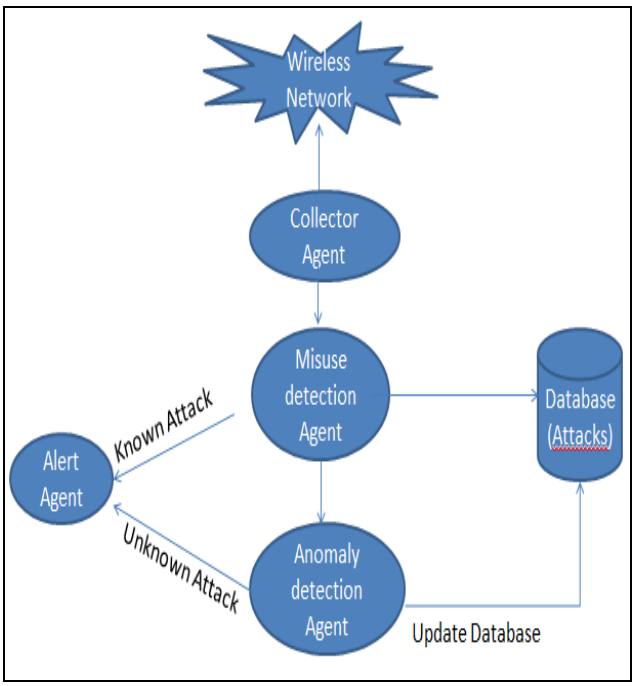


*Fig1 : System architecture*

### *4.1 System architecture*

- ***Collector Agent :***

Collector Agent is The first agent to work in the system, it collects the data from the wireless environment, store those data in a file, which is given as an input to the misuse detection agent.

- ***Misuse Detection Agent :***

Misuse Detection Agent Analyse the data captured by the collector agent. It detect the known attacks in network by pattern matching algorithm, it reports to alert agent if there is a similarity between the collected packets and attack signatures in the database,if not, those data are given as an input to the anomaly detection agent.

- ***Anomaly Detection Agent :***

Anomaly Detection Agent is used to detect the new or unknown attacks by using the classification techniques. If the incoming data is detected as attack, it report to alert agent about the attack, and update the detected attack in the database

- ***Alert Agent :***

The alert agent is used to alert the system if any intrusion occurs in the network.it alerts the system based on the output of the misuse and anomaly detection agent.

## 5. Plateform of implementation

The first major task was to choose the right technology. Many of the technologies were checked like Agent Development Kit (ADK), JADE and Aglet Software Development Kit (IBM).
These are well-known available platforms. The above mentioned technologies provide a platform for Agent development. ADK is still in its development phase and has lot of problems regarding agent movement which is the core essence of our research. JADE is FIPA compliant Agent development framework that's why it does not provide more standards for agents' mobility. Though most of the platforms have their own features and limitations but keeping in view the key property of our research, i.e. mobility, we chose MadKit platform. It provided us with the control we needed.

MadKit is a scalable and modular multi-agent platform, written in the Java language. It allows the creation of SMA based on the relational model Agent, Group, Role. MadKit leverages the Object Oriented Programming: the madKit features are contained in the kernel MadKit. This core is a set of classes for the user to design a basic way of SMA simple, but also, through inheritance, to design and add new features that will be compatible with those provided base. One of the biggest advantages is that MadKit, because it defines a basic structure for the representation of an agent, of a group, of a message. It is relatively easy to communicate with agents designed by programmers different, even for different projects.

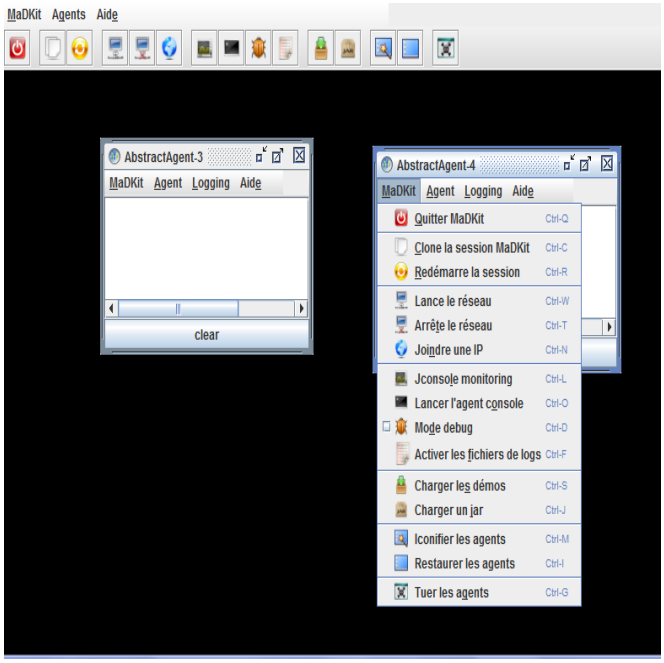


*Fig2 :MadKit Console*

The scenario for which our approach was tested is the game between two teams because it is considered a typical example of intrusion detection.We consider a game with two teams, on one side the intrusion detection system (IDS) and the other side the intruder. IDS seeks to flush out the attacks intruders protect the network. Furthermore, the intruder tries to reach its target and fulfill his plan. In intrusion detection, attack consists of several packages. The intruder reaches its target

when all the packets arrive at target. But, if the IDS arrives at intercepting a Many of these packages, the attack is then flushed out. In reality the two adversaries adopt strategies at different levels and in different ways to achieve their goals.

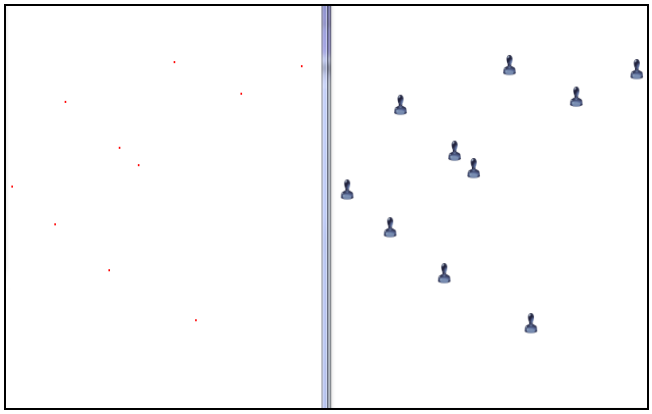

*Figure3: Representation of mobile agents*

## 6. Conclusion and future work

The proposed IDS exploits the benefits of employing mobile agents such as reduced ad hoc network bandwidth usage, increased scalability and flexibility, and ability to operate in heterogeneous environments. Here we are in position to say that mobile agents do provide a viable means of performing ad hoc network security analysis as well as some other complex tasks. As opportunities for future work, it could be identified: the deployment of a more complex detection, with mobile agents, using statistical anomalies detection identified by mobile agents and enabling the creation of attack signatures, the development of more complex detection ontology, with more parameters to characterize the attacks; the study of the impact of the use of the proposed architecture in ad hoc network traffic, and the implementation and testing of the architecture with a redundant and fault-tolerant main container.

## 7. REFERENCES

[1] DR. ZUBAIR A. SHAIKH, 'A platform independent approach for Mobile Agents to monitor Network Vulnerabilities', Proceedings of the 5th WSEAS Int. Conf. on APPLIED INFORMATICS and COMMUNICATIONS, Malta (2005).

[2] Suryawanshi G.R, S.D. Jondhale, Korde S. K., Ghorpade P.P., Bendre M.R. 'Mobile Agent for Distributed Intrusion detection System in Distributed System'(IJCTEE) Volume 1, Issue 3.

[3] J. Balasubramaniyan, J. O. G. Fernandez, D. Isacoff, E. H. Spafford, and D. Zamboni, "An Architecture for Intrusion Detection using Autonomous Agents," Technical report no. TR 98-05, Purdue University, USA, 1998.

[4] Yinan Li, Zhihong Qian, "Mobile agents based intrusion detection system for mobile Ad-hoc network" in International Conference on Innovative Computing and Communication. pp: 145-148, March 2010.

[5] N.Jaisankar, R. Saravanan, K. Duraisamy, "Intelligent intrusion detection system framework using mobile agents" in International Journal of Network Security and its Applications. Vol 1, No 2, July 2009.

[6] William M. Farmer, Joshua D. Guttman, and Vipin Swarup (1996), "Security for Mobile Agents: Issues and Requirements", In Proceedings of the 19th National Information Systems Security Conference,Vol. 2, pp. 591-597. National Institute of Standards and Technology,Baltimore, Maryland, October 1996.

[7] O.A. Ojesanmi and Ajai Crowther (2010), "Security Issues in Mobile Agents", In International Journal of Agent Technologies and Systems, Vol. 2, Issue 4, pp. 39-55, October-December 2010.

[8] Li An, Qiangfeng Jiang, Xiaoping Luo, and Zhaohui Ren (2002), "Protecting Mobile Agents Against Malicious Hosts", In CS685-002 Term Paper, Spring 2002.

[9] Niklas Borselius (2002), "Mobile agent security", In IEEE Journal of Electronics & Communication Engineering , Vol. 14, issue 5,pp. 211-218, October 2002.

[10] B. Blakley, "The Emperor's Old Armor," Proc. New Security Paradigms Wksp., 1996.

[11] R. G. Bace, Intrusion detection: Sams, 2000.

[12] R. Base and P. Mell, Intrusion Detection Systems, National Institute of Standards and Technology (NIST), Special Publication, vol. 51, pp. 800-831, 2001.

[13] K. Scarfone and P. Mell, Guide to Intrusion Detection and Prevention Systems (Idps), NIST Special Publication, vol. 8, pp. 800-894, 2007.

[14] D. Farid and M. Rahman, "Anomaly network intrusion detection based on improved self adaptive bayesian algorithm". Journal of computers, Vol. 5(1), Jan 2010, pp. 23–31, doi: 10.4304/jcp.5.1.23-31.

[15] W. Lee, S.J. Stolfo, K.W. Mok, A data mining framework for building intrusion detection models, in: Proceedings of the 1999 IEEE Symposium on Security and Privacy, Oakland, CA, USA, 1999, pp.120–132.