# Modeling an Intelligent Architecture of Intrusion Detection System for MANETs

**Sara Chadli, Mohammed Saber, Mohamed Emharraf and Abdelhak Ziyyat**

**Abstract** Mobile Ad hoc Network consists of some nodes that are stand randomly in operational environment. Because nodes are without any predefined infrastructure and mobility then there are susceptible to intrusions and attacks. Securing is an important field in this type of network. Intrusion Detection Systems (IDSs) may act as defensive mechanisms, since they monitor network activities in order to detect malicious actions performed by intruders, and then initiate the appropriate countermeasures. IDS for MANETs have attracted much attention recently and thus, there are many publications that propose new IDS solutions or improvements to the existing. In this paper, we propose a new IDS architecture for MANETs, this architecture is a combination model hierarchical based on clusters and cooperation model based on a multi-agent system (SMA). In this paper, we are used AUML language to describe the operation of different agents of our architecture.

**Keywords** Intrusion Detection System (IDS) · IDS architectures · Mobile ad hoc networks (MANETs) · AUML · Multi-Agent System (SMA) · MANETs security · Security attacks

S. Chadli (✉) · A. Ziyyat
Laboratory Electronics and Systems, Faculty of Sciences, First Mohammed University,
Oujda, Morocco
e-mail: chad.saraa@gmail.com
URL: http://www.ump.ma

A. Ziyyat
e-mail: abdelhak_ziyyat@hotmail.com

M. Saber · M. Emharraf
Laboratory LSE2I, National School of Applied Sciences, First Mohammed University,
Oujda, Morocco
e-mail: mosaber@gmail.com

M. Emharraf
e-mail: m.emharraf@gmail.com

A. El Oualkadi et al. (eds.), *Proceedings of the Mediterranean Conference on Information & Communication Technologies 2015*, Lecture Notes in Electrical Engineering 381, DOI 10.1007/978-3-319-30298-0_57

# 1 Introduction

A mobile ad hoc network (MANET) is a collection of autonomous nodes that form a dynamic, purpose-specific, multi-hop radio network in a decentralized fashion. The wireless mobile natures of MANETs in conjunction with the absence of access points, providing access to a centralized authority, make them susceptible to a variety of attacks [1]. An effective way to identify when an attack occurs in a MANET is the deployment of an Intrusion Detection System (IDS).

The existing IDS architectures for MANETs fall under three basic categories [2, 3] (a) stand-alone, (b) cooperative and (c) hierarchical. The employed intrusion detection engines are also classified into three main categories [4]: (i) signature-based; (ii) anomaly-based engines and (iii) specification based engines.

In this paper, we have proposed a hybrid model of intrusion detection system which combines between models hierarchical based on of clusters and cooperation model based on a multi-agent system (SMA. The rest of this chapter is organized as follows. Section 2 we present in detail the design of proposed architecture. Section 3, we present in detail the operating of proposed architecture. Finally, Sect. 4 contains the conclusions.

# 2 Proposed IDS Architecture for MANETs

In this section we present our IDS architecture for MANETs. First, we include the objectives of our classification, and then we present the design of our architecture.

## *2.1 Design of Our IDS Architecture for MANETs Based on Multi-agent*

Our architecture is a combination of hierarchical model based of clusters and cooperative model based on a multi-agent system. The Clustering in MANETs is an effective way to structure the network. Its purpose is to identify a subset of nodes (Fig. 1a) in the network and assigned him a the designated node (DN).

The node is elected by applying the clustering algorithm HEED (Hybrid, Energy-Efficient, Distributed) [5], because this algorithm has four primary objectives: (i) prolonging network lifetime by distributing energy consumption, (ii) terminating the clustering process within a constant number of iterations, (iii) minimizing control overhead (to be linear in the number of nodes), and (iv) producing well-distributed cluster heads.

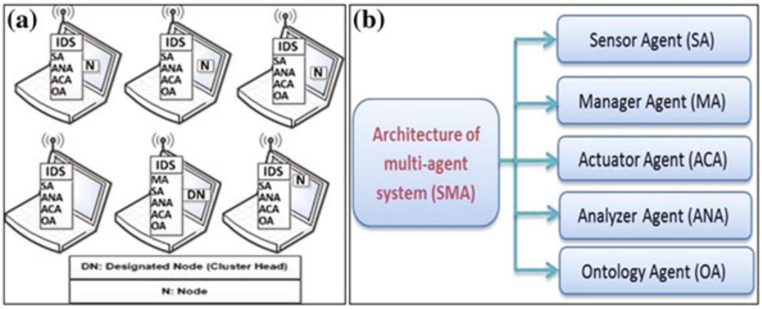

**Fig. 1** **a** Architecture of Cluster in MANET; **b** architecture of multi-agent system

In our proposed architecture, the agents realizing detection tasks by communication and collaboration between them. The architecture consists of a multi-agent detection system that uses five classes of agents (Fig. 1b): Sensor Agent (*SA*), Manager Agent (*MA*), Ontology Agent (*OA*), Agent actuator (*ACA*) Agent Analyzer (*ANA*).

## 2.2 Design of a MANET Node in Our Architecture

In our architecture, the agents (SA), (ANA) (ACA) and (MA) are installed in the various Member nodes of MANET cluster. The designing a node based agents as shown in (Fig. 2).

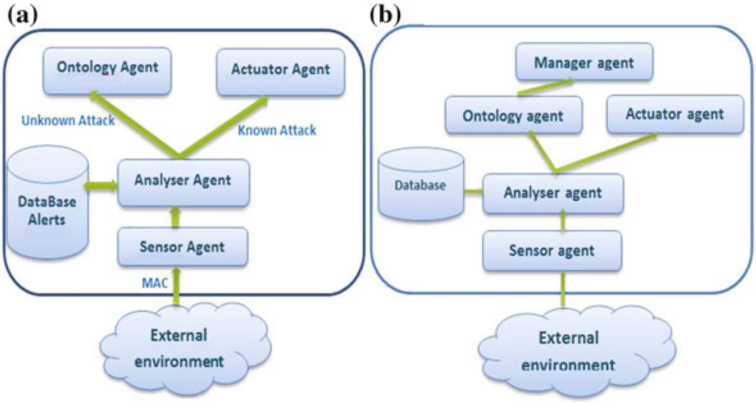

**Fig. 2** **a** IDS Architecture node in SMA; **b** IDS architecture of cluster head in SMA

## 3 Operation of Our Architecture

Our model of security and intrusion detection based on a distributed approach using multi-agent system for receiving intelligence of these agents. It is formed by agents with the capacity to react quickly reactive against different types of attacks (Fig. 3).

To facility the operation of our proposed model of multi-agent system we are used design based on the AUML language for describing the operation of agents as follows.

### 3.1 Sensor Agent(SA)

The sensor agent (SA) *Sensor()*, is the initiator of the detection process. It is down the chain of operation, it captures network raw traffic by using functions *get_info()* and *get_origin()*, and formate in a predefined format by using *set_format()* function that will be sent to the agent analyzer (ANA) with *Send_analyser* function. The

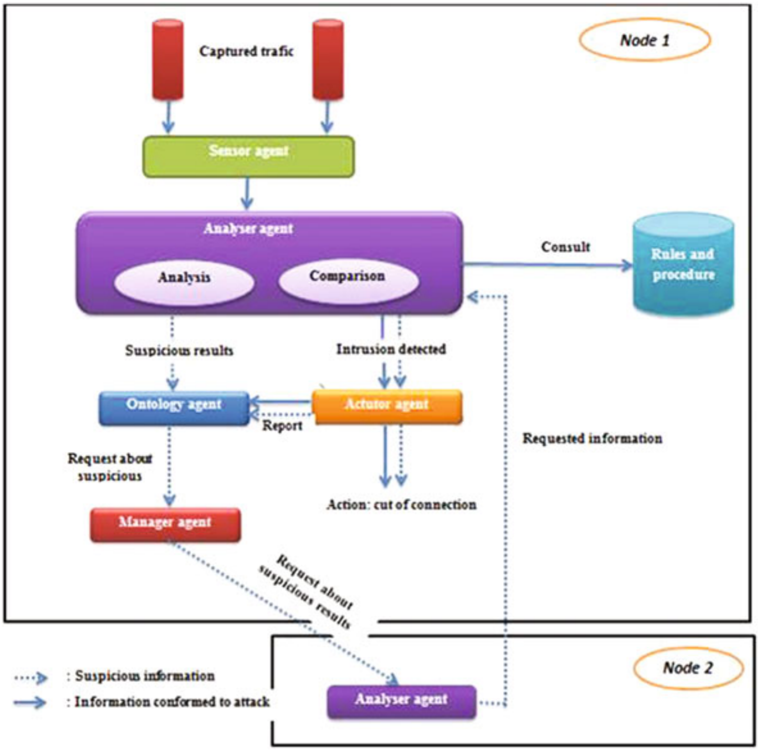

**Fig. 3** Schematic of the intrusion detection platform proposed

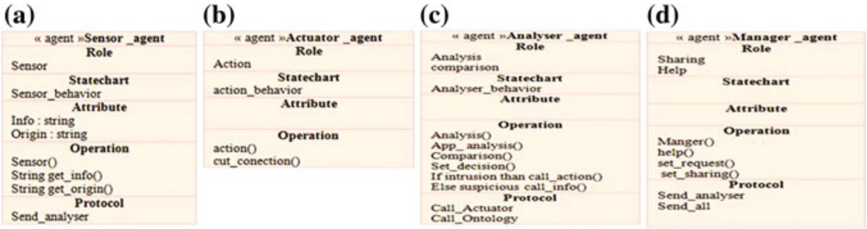

**Fig. 4** Implementation level of the: **a** Sensor Agent; **b** Actuator Agent; **c** Analyzer Agent; **d** Manager Agent

following figure (Fig. 4a) shows a portion of the class agent diagram for the agents sensor.

## 3.2 Analyzer Agent(ANA) and Actuator Agent (ACA)

The analyzer agent *analyser()* analyse the formatted data with *app_analysis()* function and compare the analysis result by applies rules of detection recorded in his database with *comparison()* and *set_decision()* functions (Fig. 4c). According to the analysis result, this agent will initiate an external treatment. Two cases are possible:

- If a malicious activity is confirmed an attack signature, then the analyzer agent use *call_action()* function and *call_actuator()* functions to communicates the result to the actuator agent to perform the necessary actions by using *action()* and *cut_connection()* functions (Fig. 4b).
- In second case if the activity is judged suspicious by comparison of detection thresholds, the agent analyzer (ANA) request additional information to confirm the nature of the activity we say that it is initiating agent collaboration. The analyser agent send request to ontology agent by using *call_ontology()* function to offers semantic verification service of the knowledge to facility the operation for other agent the following figures (Fig. 4b) show a portion of the class agent diagram for the Analyser agent and actuator agent.

## 3.3 Manager Agent(MA)

The manager agent can ask other agents for local information related to suspicious activity with *help()* and *get_request()* functions, in this case one or more agents analyzer located in different nodes in cluster can provide local information to the initiator. In this case one or more agents analyzer located in different nodes in cluster can provide local information to the initiator. This last will repeat the same operation as we see in first case. For its part the manager agent can invoke a data sharing with *set_sharing()* and *send_all()* functions to enrich local data at the initiator. The following figures (Fig. 4d) show a portion of the class agent diagram for Manger agent.

## 4 Conclusion

In this paper we did a study the IDS architectures for MANETs and we have proposed a hybrid model of intrusion detection system which combine between model hierarchical based on of clusters and cooperation model based on a multi-agent system (SMA). Our new architecture is distributed architecture based on the intelligence of the multi-agent system allowing both to reacting rapidly against complex attacks and evaluating the state of flows relative to predefined rules and procedures and other hand enhances the level of security provided to the target monitored.

In the future, after the design phase of the proposed model, we think to use an open source platforms (JADE and MADKIT) to develop the new system intrusion detection and we conducted a simulation platform that reflects the goals already set.

## References

1. Chadli, S., Saber, M., Ziyyat, A.: Defining categories to select representative attack test-cases in MANETs. In: IEEE Xplore DIGITAL LIBRARY, pp. 658, 663 (2014). doi:10.1109/CSNT.2014.138
2. Anantvalee, T., Wu, J.: A survey on intrusion detection in mobile ad hoc networks, wireless/mobile network security Springer (2006) Chapter 7, pp. 170–196. Wireless Network Security. doi:10.1007/978-0-387-33112-6_7
3. Xenakis, C., Panos, C., Stavrakakis, I.: A comparative evaluation of intrusion detection architectures for mobile ad hoc networks. Comput. Secur. **30**(1), 63–80 (2011). doi:10.1016/j.cose.2010.10.008
4. Li, Y., Qian, Z.: Mobile agents-based intrusion detection system for mobile ad hoc networks. In: 2010 Intl Conf on and Information Technology & Ocean Engineering Innovative Computing & Communication, 2010 Asia-Pacific Conf on (CICC-ITOE), pp. 145, 148, 30–31 Jan 2010. doi:10.1109/CICC-ITOE.2010.45
5. Younis, O.; Fahmy, Sonia, HEED: a hybrid, energy-efficient, distributed clustering approach for ad hoc sensor networks. IEEE Trans. Mob. Comput. **3**(4), 366, 379. doi:10.1109/TMC.2004.41