A Security Response Approach Based on the Deployment of Mobile Agents

Roberto Magán-Carrión, José Camacho-Páez, and Pedro García-Teodoro

Department of Signal Theory, Telematics and Communications,
Faculty of Computer Science - CITIC, University of Granada
{rmagan,josecamacho,pgteodor}@ugr.es

Abstract. This paper introduces a response mechanism to improve the tolerance against security threats in MANET environments. The mechanism is started after detecting the existence of nodes with malicious behavior, and is based on the use of one or more mobile agents to improve the connectivity of the network. This way, in the event of the detection of a malicious node (e.g. a *selfish* node or a *dropper* node), an agent is employed to maximize the overall connectivity of the network. Every agent acts as a relaying node within the MANET and it is automatically positioned according to a particle swarm optimization (PSO) process. This paper represents a work in progress. However, the promising results obtained show the good suitability of the approach to improve the survivability of the network from a security perspective.

Keywords: agent, PSO, detection, malicious, MANET, response, survivability, tolerance.

1 Introduction

In the context of ad hoc networks, mobile ad hoc networks (MANET) have a several special characteristics: lack of a fixed infrastructure, dynamic changing topology, resource constraints and limited physical security, among others [1]. In this kind of networks, the communication between nodes is restricted and depends of their coverage range. Therefore, not all the nodes are directly connected, and thus a multi-hop relay-based scheme is needed for end-to-end transmissions. Some possible applications of MANETs include military scenarios, e.g. soldier communications in the battlefield; emergency rescue, e.g. earthquake or fire disasters when the fixed communication infrastructures are no longer available.

Compared with traditional wired networks, MANETs are much more vulnerable to attacks due to the limited energy of nodes, thus avoiding the use of complex security solutions, the wireless transmission medium, which makes eavesdropping easier, the lack of management and control unit and the implicit mobility of these environments. Attacks like *blackhole*, *sinkhole*, *dropping* or malicious behaviors as *selfish*, are specific for MANETs [2]. These inherent threats have an obvious and high impact over the network performance, since nodes need to send information through intermediate neighbors that could be attackers. Thus, security mechanisms to strengthen the services provided are needed.

Y. Demazeau et al. (Eds.): PAAMS 2013, LNAI 7879, pp. 182–191, 2013.

Deploying efficient security systems to reduce risks and threats by providing proper mechanisms to maximize the network performance is also required. This will raise the network survivability, which is defined as *"the ability of a system to fulfill its mission, in a timely manner, in the presence of attacks, failures or accidents"* [3].

In this context, the present work proposes a multiagent-based system aimed at enhancing the connectivity between nodes in the network in the presence of nodes with malicious behaviors. Hence, a tolerant and resilient network is obtained. The response mechanism presented here is based on the work of *Dengiz et al.* [4], where the authors improve the network performance by maximizing the connectivity and the amount of flows transmitted. They make use of the particle swarm optimization (PSO) algorithm and the future user node locations (kinematic predictions), to situate the agent nodes in optimal positions to maximize the overall connectivity.

The principal contribution of this paper is the use of mobile agents as a response mechanism for improving security in MANETs. This way, in the event of the detection of malicious nodes in the environment, the corresponding worsening of the network performance is mitigated by deploying some agents in charge of relaying packets and thus improving overall coverage and connectivity. Even though this paper represents a work in progress, and thus much more experimentation is in due, the preliminary experimental results obtained show the promising performance of our approach.

The rest of the paper is organized as follows. Section 2 presents some relevant works about multiagent systems in general, and security related ones in particular. Section 3 introduces a discussion about the reference work and the novel system proposed here. Some experimental results and simulation to corroborate and validate the system efficacy are described in Section 4. Finally, Section 5 summarizes the principal conclusions and remarks of this work as well as future research directions.

2 Related Work

There are several proposals in the literature on the use of mobile agents in ad hoc wireless networks addressing different kinds of challenges: network connectivity and node optimization positioning, improvement of network QoS parameters, energy optimization and security issues. In [5] the locations of agent nodes are optimized by means of a PSO algorithm to maximize the connectivity between user nodes and a control node. A PSO algorithm is also used in [4] enhanced with a kinematic prediction of user nodes motion following the scheme of model predictive control (MPC), with the aim of maximizing the connectivity and flow transmission in MANETs. Furthermore, in military scenarios, a supervisor mobile agent trajectory is optimized according the deployed positions of the user nodes, thus maximizing the connectivity between the control node and the arranged user nodes [6].

Ant colony optimization (ACO) and bee colony optimization (BCO) algorithms are used to improve QoS parameters and for energy optimization. Packet delivery ratio and end-to-end delay are the focus in [7]. In that reference, an ACO scheme is used to find out the shortest path both in routing discovery and maintenance phases. Similarly, the authors in [8] improve the network bandwidth by using an ACO algorithm. Here, a number of ants are in charge of discovering the best routes according to the destination distance, the available bandwidth and the queue of the nodes. An efficient routing algorithm is proposed in [9], where the routes are selected by employing bees to select the path with least energy consumption requirements.

Deploying attack detection (recognition) and event response (recovery) mechanisms constitute key issues for network survivability [3]. Non-legitimate event detection in networks is an aspect that has been recurrently studied in the specialized literature. On the other hand, response mechanisms try to solve the non-legitimate events detected in order to guarantee the continuity of the network and the affected services. Nevertheless, in the multiagent system field just a few works have been developed to address security detection and response issues, and these are limited to the use of software agents. In [10] an agent node is created and sent from the sender to the destination crossing the suspected node. If the agent never comes back, the suspected node is concluded to be a *grayhole* or a *blackhole* node. Unlike the previous work, in [11] the agent records the amount of packets received and forwarded by each node along the path. If the agent detects that the forwarded and received packets ratio is under a fixed threshold, the node is labeled as malicious. Then, a report is sent to the sender. A scheme imitating the human immune system is proposed in [12]. There exists an immune agent (IA) that is distributed along the network. The IA is in charge of detecting, classifying, isolating, and recovering if needed. A node that exceeds a certain number of attacks launched will be isolated. Reference [13] introduces a similar scheme, where the nodes are monitored and, if necessary, isolated by using two types of mobile agents: detection agent and counterattack agents. The first ones are in charge of detecting malicious behaviors, while the second ones will surround and isolate the invaders. In [14] the dynamic source routing protocol (DSR) for MANETs is modified by attaching two agents to each network node: a monitoring agent (MOA) and a routing agent (ROA). The first one monitors the node behavior to assign a trust value. The trust values are spread throughout the network into the route request packets. Afterwards, the ROA agent selects the trustworthiness route discarding others with less trust level. Thus, the nodes with low trust value are isolated.

In what follows we propose the use of physical and mobile agents as a response mechanism. Based on the pre-existence of a detection module for malicious behaviors, our approach consists of the deployment of one or more agents to solve the loss of “coverage” due to malicious nodes. The agents, acting as relaying nodes, will allow to improve the overall connectivity of the network.

3 MARS: Mobile Agent Response System

As mentioned above, the proposed system is inspired by the work of *Dengiz et al.* work [4], in which the connectivity of a MANET is improved by using mobile agent nodes. In this section, a brief explanation of that approach is first presented. A description of the specific response system proposed here, named MARS, is afterwards provided.

3.1 Connectivity Maximization Using PSO and Future Motion Predictions

Two types of nodes are involved in [4]: user nodes and agent nodes. User nodes are final nodes demanding some given network service, while agent nodes try to guarantee that user nodes are receiving the best network service as possible by maximizing the overall connectivity. The connectivity is related to the coverage range. Two nodes are accessible or connected (that is, there is a link between them) if the Euclidean distance between them is less or equal to R, where R is the coverage range of a radio node.

Basically, the authors in [4] suggest two objectives: to maximize the overall connectivity of the network, and to optimize the flow transmission. This optimization process is achieved by using the PSO algorithm [15] and several optimization functions. Two important and particular entries of the PSO algorithm are: the future motion predictions of user nodes for a specific prediction time horizon $(t + H)$, and the best solution previously obtained. Afterwards, a comparison among several possible problem solutions (*particles*) is made. The different particles in the same PSO run are specific network distributions where the user node locations at $t + H$ are the same and the agent nodes positions are modified by increasing or decreasing its velocity and direction values. When the PSO optimization process is finished, the algorithm returns the best locations of each agent node to maximize the overall connectivity and flow transmission of the network at a given time instant.

There are three optimization functions involved. With the first, O_1, the global network connectivity is evaluated. This can be obtained from:

$$O_{1t} = \frac{2 \times \sum_{i,j \in UN_t : j > i} Z_{ijt}}{UN \times (UN - 1)} \tag{1}$$

where UN is the number of user nodes and $Z_{ijt} = 1$ if there exists an available (either single or multi-hop) path connecting the ith and jth user nodes at time t. Otherwise, $Z_{ijt} = 0$.

A second function, O_2, maximizes the flow transmission by improving the weakest link, in flow terms, of the network, which will enhance the overall network performance. O_2 is only evaluated when several possible solutions of the optimization (several particles under evaluation) represent completely connected networks, that is if $O_1 = 1$ in all of them. For disconnected networks, a third function O_3 is considered, which measures the distance from each agent to the imaginary middle point between non connected partitions of the network. In summary, the solution with a higher O_1 value is the best solution. If there are several completely connected networks in the solution of the optimization, the one with higher O_2 value is selected. However, if there are disconnected networks with the equal O_1 values, the one with lower O_3 value is chosen.

The optimization algorithm is iteratively repeated over the time, the agents being dynamically positioned at their best locations step by step. More details about the entire process can be found in the reference paper [4].

3.2 System Description

As commented in Section 2, there are few research proposals about response solutions in MANET networks, specially involving multiagent systems. Instead, most of them are merely related to the detection of malicious behaviors.

In this context, MARS is intended to establish a response mechanism for security alarms in MANETs by using mobile agents. MARS is conceived to be a tolerant mechanism against attacks such as *selfish*, where a node has an egoistic behavior not forwarding packets to preserve its own resources (e.g. battery life); or *dropping*, where a node drops the received packets instead of forwarding them.

Both types of attack, *selfish* and *dropping*, among others, have similar consequences on network performance. This way, these kinds of malicious nodes will prevent other nodes to communicate with each other. Using MARS, such attacks can be dealt with:

1. A monitoring system is deployed to detect this kind of behaviors. See [16] for an example of such a system. The design of the monitoring system is out of the scope of this paper.
2. Once one or more malicious nodes are detected, the MARS response mechanism is triggered. A set of mobile agents are dynamically launched, which present two main features. First, they act as mere relaying nodes to solve the decrease in connectivity in the network due to the appearance of malicious nodes. Second, the base optimization algorithm proposed in [4] is executed to determine the best positions of the agents to maximize the overall connectivity over the time.

To illustrate how MARS works, Figure 1 depicts different network situations. Initially, several user nodes (solid circles) are randomly distributed throughout a given network area, where there is also one malicious node (inverted triangle) and one agent node (solid square). At the beginning, in Figure 1(a), the malicious node works as a normal node. Afterwards, in Figure 1(b) the attack is in progress, so that the overall connectivity is broken and two separated networks are obtained. Figures 1(c) and 1(d) show the coverage recovery process. The agent, A1, is approaching to its optimal position (according to PSO), thus making possible the connection among the previously disconnected user nodes. In this case, the use of one single agent cannot provide full connectivity between user nodes due to their motion and the coverage range. Nevertheless, the position of A1 is optimally computed in order to connect the maximum number of nodes, as shown in Figures 1(e) and 1(f).

4 Experimental Results

This section is devoted to study the performance of our security response/tolerance system. For that, a set of experiments in a simulation scenario with Matlab are carried out. The main features of the scenario are:

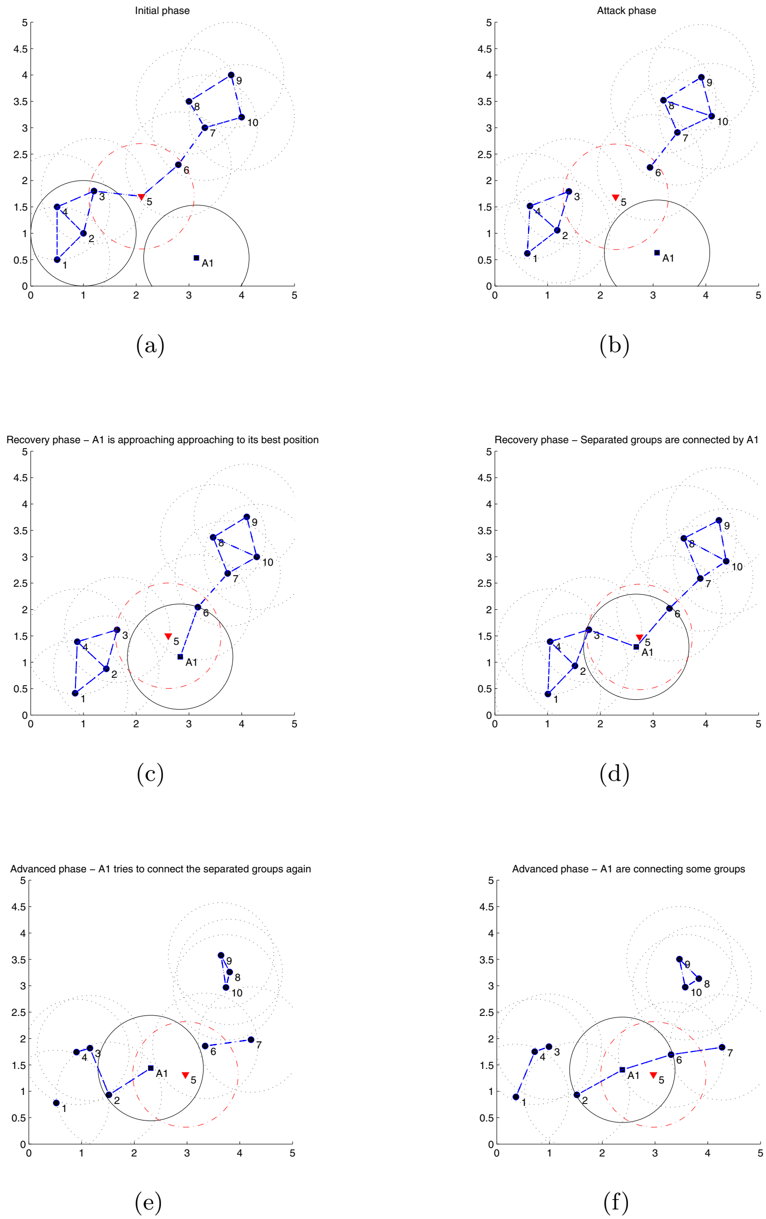
1. The network area is 5m × 5m.
2. The coverage range R=1m, thus assuring disconnection among nodes.
3. The prediction horizon H=4, because it is an optimal value that offers better connectivity values in accordance with [4].

In order to evaluate the evolution of the connectivity of the network under various situations with respect to the number of final user nodes (UNs), number of malicious nodes (MNs), and number of agent nodes (ANs), ten different combinations are proposed:

1. With no attacks, that is under normal operation of the user nodes. In this case, we are going to obtain the connectivity for 10, 20, 30 and 40 UNs.
2. In the presence of attacks. In this case, the connectivity is obtained for 40 UN, while the number of MNs is taken to be equal to 1, 5 and 10.
3. With attacks and ANs to solve them. The study of the connectivity is done for 40 UNs, 10 MNs and the number of ANs equals to 1, 5 and 10.

Each connectivity analysis involves 25 repetitions for each experiment, where different initial random distributions of UNs and ANs in the network area are considered. Figures 2, 3 and 4 show the results obtained from our experimentation. As expected, O_1 increases in Figure 2 with the number of user nodes, since effective links will be established among them due to the fact that the global area size does not change. In other words, UNs are nearer to each other. The negative effect of the MNs in the network connectivity is illustrated in Figure 3, which shows how this connectivity decreases as the number of MNs increase. Finally, Figure 4 shows that the deployment of ANs in the environment, once the MNs are identified, contributes to the recovery of the connectivity of the overall network. On the one hand, the connectivity increases with the number of ANs. On the other hand, the connectivity with 10 ANs and 10 MNs is even higher than when there is no MNs in the MANET. This shows the effectiveness of the approach, and it is the result of the optimization of the ANs location.

Figure 4 shows that the deployment of ANs in the environment, once the MNs are identified, will contribute to recover the connectivity of the overall network. On the one hand, the connectivity increases with the number of ANs. On the other hand, it is important to remark the fact that the overall connectivity of a network for a given number of user nodes plus agent nodes is higher than when all the nodes are user nodes. The reason for that is simple, since the ANs are intelligent in the sense that they try to be positioned to maximize the global connectivity.



(a)

(b)

(c)

(d)

(e)

(f)

Fig. 1. Connectivity maximization and recovery process. Initial phase where a malicious node (inverted triangle) is performing the forwarding process together with the user nodes (solid circles) (a). Two separated groups of nodes result when the attack is carried out (b). Motion of the agent A1 when approaching to its optimal location recover connectivity and thus communications (c) (d). The agent is finally positioned to connect the maximum number of nodes (e) and (f).

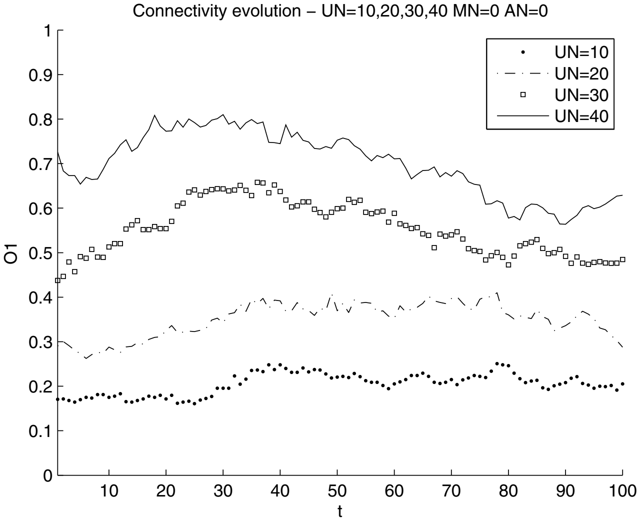


Fig. 2. Connectivity evolution along 100 time instants in normal conditions without influence of attacker or agent nodes. As expected, the connectivity increases as the number of user nodes, UN, becomes higher.

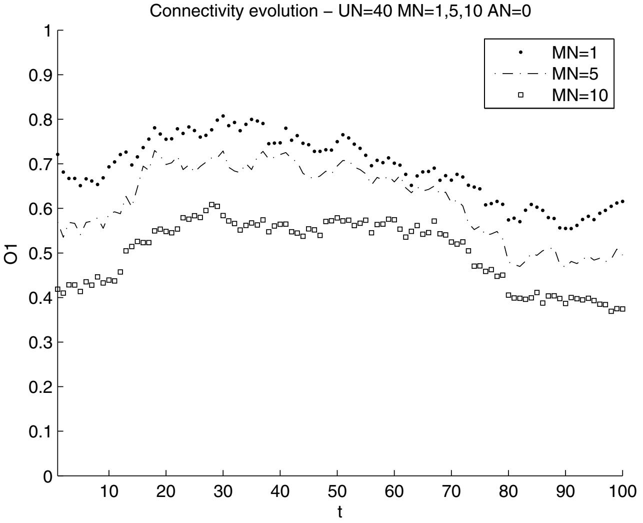


Fig. 3. Connectivity evolution along 100 time instants under influence of attacker or malicious nodes (MN). As expected, the connectivity becomes lower as the number of MNs increases.

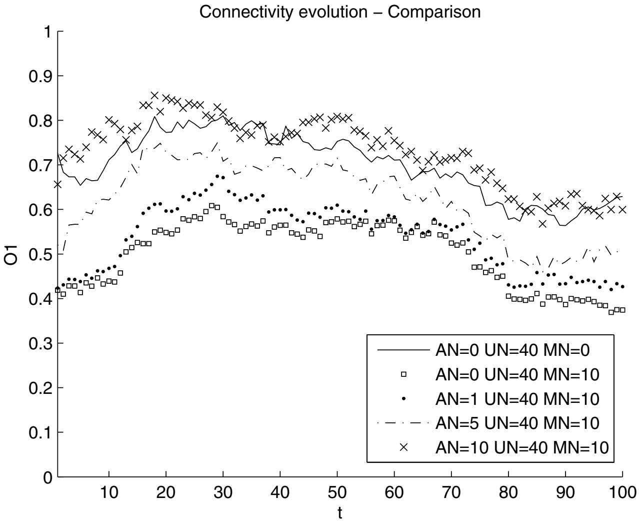


Fig. 4. Connectivity evolution along 100 time instants under influence of both malicious and agent nodes. The agents contribute to improve the connectivity, so it is raised as the number of ANs does. Also a comparison with two previous cases is done, in order to show the connectivity improvements gained by the agent nodes position optimization.

5 Conclusions and Future Work

In this paper a novel response/tolerance approach for security threats in MANETs is proposed. It is based on the use of mobile agent nodes, which are launched after detecting the existence of malicious nodes in the environment that decrease the connectivity of the network. A positioning optimization procedure is carried out to determine the best positions of agents over the time.

The experimental results obtained show the improvement in connectivity and thus the tolerance and survivability exhibited by the network operation when confronted to security attacks, when our approach is considered. Nevertheless, further work should be performed to strengthen the current proposal. Some issues may be mentioned in this line. First, alternative parameters to that of connectivity may lead the positioning of the nodes depending on different objectives established for the network. Second, the agent nodes can operate in different ways depending of other various types of attacks. Third, the response/tolerance scheme could be used as a feedback element to strengthen the security design of the network.

Acknowledgment. This work has been partially supported by Spanish MICINN through project TEC2011-22579 and by the FPU P6A grants program of the University of Granada.

References

1. Wu, B., Chen, J., Wu, J., Cardei, M.: A Survey of Attacks and Countermeasures in Mobile Ad Hoc Networks. Springer, US (2007)
2. Ehsan, H., Khan, F.A.: Malicious AODV: Implementation and Analysis of Routing Attacks in MANETs. In: Procedings of the 11th IEEE International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom 2012), UK, pp. 1181–1187 (June 2012)
3. Lima, M., dos Santos, A., Pujolle, G.: A survey of survivability in mobile ad hoc networks. IEEE Communications Surveys & Tutorials 11, 66–77 (2009)
4. Dengiz, O., Konak, A., Smith, A.E.: Connectivity management in mobile ad hoc networks using particle swarm optimization. Ad Hoc Networks 9, 1312–1326 (2011)
5. Cho, Y., Smith, J.S., Smith, A.E.: Optimizing tactical military MANETs with a specialized PSO. In: 2010 IEEE Congress on Evolutionary Computation (CEC), pp. 1–6. IEEE (2010)
6. Miles, J., Kamath, G., Muknahallipatna, S., Stefanovic, M., Kubichek, R.F.: Optimal trajectory determination of a single moving beacon for efficient localization in a mobile ad-hoc network. Ad Hoc Networks (2012)
7. Asadinia, S., Rafsanjani, M.K., Saeid, A.B.: A novel routing algorithm based-on ant colony in Mobile Ad hoc Networks. In: 2010 3rd IEEE International Conference on Ubi-media Computing (U-Media), pp. 77–82. IEEE (2010)
8. Daniel, A.K., Singh, R.: Swarm Intelligence Based multicast Routing and Bandwidth Management protocol for Ad-hoc wireless Network Using Backpressure Restoration. In: 2010 3rd IEEE International Conference on Computer Science and Information Technology (ICCSIT), vol. 5, pp. 516–520. IEEE (2010)
9. Fahmy, I.M.A., Hefny, H.A., Nassef, L.: PEEBR: Predictive Energy Efficient Bee Routing algorithm for Ad-hoc wireless mobile networks. In: 2012 8th International Conference on Informatics and Systems (INFOS), pp. NW-18–NW-24. IEEE (2012)
10. Taggu, A., Taggu, A.: An application-layer scheme for intrusion detection in MANET using mobile agents. In: 2011 Third International Conference on Communication Systems and Networks (COMSNETS), pp. 1–4. IEEE (2011)
11. Roy, D.B., Chaki, R.: Detection of Denial of Service Attack Due to Selfish Node in MANET by Mobile Agent. In: Özcan, A., Zizka, J., Nagamalai, D. (eds.) WiMo/CoNeCo 2011. CCIS, vol. 162, pp. 14–23. Springer, Heidelberg (2011)
12. Mohamed, Y.A., Abdullah, A.B.: Immune-inspired framework for securing hybrid MANET. In: IEEE Symposium on Industrial Electronics Applications, ISIEA 2009, vol. 1, pp. 301–306. IEEE (2009)
13. Ye, X., Li, J.: A security architecture based on immune agents for MANET. In: International Conference on Wireless Communication and Sensor Computing, ICWCSC 2010, pp. 1–5. IEEE (2010)
14. Halim, I.T.A., Fahmy, H.M.A., Bahaa El-Din, A.M., El-Shafey, M.H.: Agent-Based Trusted On-Demand Routing Protocol for Mobile Ad Hoc Networks. In: 2010 4th International Conference on Network and System Security (NSS), pp. 255–262. IEEE (2010)
15. Eberhart, R., Kennedy, J.: A new optimizer using particle swarm theory. In: Proceedings of the Sixth International Symposium on Micro Machine and Human Science, Nagoya, pp. 39–43 (1995)
16. Sánchez-Casado, L., Maciá-Fernández, G., García-Teodoro, P.: An Efficient Cross-Layer Approach for Malicious Packet Dropping Detection in MANETs. In: Procedings of the 11th IEEE International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom 2012), UK, pp. 231–238 (June 2012)