RAIRO-Oper. Res. 50 (2016) 285–296
DOI: 10.1051/ro/2015047

RAIRO Operations Research
www.rairo-ro.org

SECURITY MODELING OF AN *AD HOC* NETWORK UNDER THE CONSTRAINT OF ENERGY BY AN APPROACH IN TWO STEPS: CLUSTERING-EVOLUTIONARY GAME

Karima Adel-Aissanou[1], Sara Berri[1], Myria Bouhaddi[1] and Mohammed Said Radjef[1]

Abstract. *Ad hoc* networks are subject to multiple challenges, particularly the problem of limited resources such as energy and vulnerability in terms of security. Indeed, the nodes are subject to various attacks and malicious actions. Thus, each mobile is confronted with a dilemma: cooperate to ensure security, in this case the node spend a part of its energy, or not cooperate which allows it to save energy but making the security of the network more vulnerable. In this work, we develop an approach which takes into account two conflicting objectives: contribute to network security while reducing energy consumption. The approach is based on alternating two steps: Clustering-Evolutionary game. The clustering step is performed by an algorithm that takes into account the energy constraint in election of cluster-heads. The interactions between each pair of cluster-heads, when exchanging data, in their contribution to the security of the network, are modeled as an evolutionary game which is the second step of the proposed approach.

Mathematics Subject Classification. 90B18, 91A22, 91C20, 91A10, 91A80.

Received September 12, 2015. Accepted September 28, 2015.

1. Introduction

In recent years, the need for more mobility and share or exchanging information at any time have given rise to new technology of mobile wireless networks called *Ad hoc* networks. These networks are composed of a set of mobile nodes, which move and communicate autonomously by radio waves and are self-organizing and self-administering without a fixed infrastructure [1,6].

When the number of nodes is very important, the management of the network becomes very difficult. One solution is to divide the network to subsets called clusters. Each cluster will then be identified by its cluster-head, which will act as a local coordinator in the cluster. The cluster-head election is according to a given criterion.

Several clustering algorithms have been proposed in the literature and they are distinguished by the selection criteria of cluster-heads. Some algorithms chose simple criteria, such as identifying (ID) [5], the connectivity

Keywords. Ad hoc networks, security, clustering, evolutionary games, replicator dynamic, convergence, simulation.

[1] Research Unit of LaMOS (Modeling and Optimization of Systems), Faculty of Exact Sciences, University of Bejaia, 06000 Bejaia, Algeria. ak_adel@yahoo.fr; berri.sara2012@gmail.com; myria.bouhaddi@gmail.com; radjefms@yahoo.fr

degree [12]. Other approaches adopted more sophisticated selections based on a combination of criteria such as (WCA) [8]. In [2], the authors summarize works about clustering algorithms in *Ad hoc* networks.

The clustering has also the effect of preserving the nodes energy which is a key in the network life time and several works were made in this direction [11, 20].

Ad hoc networks can be targets for many attacks that can cause damage and thus degrade their performance. The mobility of nodes and the absence of centralized infrastructure make the use of security mechanisms, developed for wired networks, impossible. All these constraints make the security of *Ad hoc* networks very complex and difficult to guarantee. In the literature, we can find different approaches to modeling and solving these problems, among which we find those using game theory [3, 4, 10, 16, 19, 21, 22].

To counter the attacks against network, all its composing nodes must be equipped with an IDS[2]. Thus, a situation of interaction is created between the IDS, whose purpose is to protect the network, and the attacker which tries to compromise the network security.

The authors in [10, 21] modeled the interactions between an attacker and an IDS as a Bayesian game. The attacker tries to create the most damage in the network without being detected, while the defender tries to maximize its defense capabilities. The authors in [10] considered both the static and the dynamic game. In the static game, results are mixed and pure Bayesian Nash equilibria, and in the dynamic one, it is the perfect Bayesian equilibrium in mixed strategies. In [21], the authors' aim is to reduce energy consumption caused by the continuous activation of the IDS. The analysis of the results given by the model show that the activation of the IDS may be done intermittently without compromising its effectiveness.

As the attacks and defenses change the state of the network, another modeling was presented in [22] as a non-zero-sum stochastic game. The authors in [22] calculated the Nash equilibrium and explained how to use these results to improve network security. In [19], unlike other works, the attacker is formed by a collaborative group of malicious nodes called malicious coalition. The authors in [3] presented a comparison between different approaches to the problem of security in an *Ad hoc* network based on game theory. They thus presented the advantages and disadvantages of each of them.

In all these models, the main goal of the attacker is to choose strategies causing more damage to the network while the defender tries to minimize them. The goal of the attacker and the defender are strictly opposed. Thus, in [4], the zero-sum game is used to model the security of the network. Other models [16] relax the hypothesis of rationality of players assumed in the classical game theory, and use evolutionary game theory for modeling the security.

In most of these studies, it is assumed that all nodes are control nodes, *i.e.* the IDS of each node is activated, which is not very judicious in terms of energy consumption which is a key factor in the network lifetime. To deal with the security problem in *Ad hoc* network while reducing the energy consumption of all the nodes, we provide in this paper a fundamentally cooperative approach. The idea is to activate the IDS only on a limited number of nodes as it was done in [7, 15]. We consider the set of cluster-heads which were elected according to a criterion that takes into account the energy level. Thus, the role of cluster-heads is to ensure the safety of their cluster, taking into consideration that some of them may not accomplish their control task by not activating their IDS. To see the state evolution of the network resulting from the behavior of nodes selected to ensure the control of traffic in the network, we develop an approach based on evolutionary game theory by referring to the model proposed in [16]. This class of games is chosen because of the low rationality of nodes. This category of games also allows to model the dynamic evolution of a population of interacting individuals using two fundamental concepts: the evolutionary stable strategy (ESS) and the replicator dynamic.

The rest of this paper is organized as follows: in Section 2, we present the problem setting and modeling. We give the main algorithm in section 3. Section 4 is devoted to present simulation results, performance evaluation and comparative study of our model. We give concluding remarks in Section 5.

[2]IDS (Intrusion Detection System): Process of monitoring events within a network, it allows to detect in real-time and in continuous way the intrusion attempts.

2. The model

We consider the problem of security of an *Ad hoc* network composed of a number of nodes. The approach that we develop in this paper is based on the alternation of two steps:

- clustering, in order to distribute the nodes into clusters and to elect for each one the cluster-head;
- modeling the interactions between cluster-heads by an evolutionary game, in which players strategies are to contribute or not to the network security by activating or deactivating their IDS.

2.1. Step of clustering

Besides energy and security, the connectivity is an important characteristic of an *Ad hoc* network which should not neglect in a study. In this kind of networks, each node contributes to the connectivity of the entire network. Indeed, when the number of nodes is important, maintain this connectivity becomes a hard problem. The clustering is one of solutions adopted in the literature. High-Connectivity Clustering (HCC) [12] is one of algorithms using connectivity criteria for the election of the cluster-heads. In our work, we take the same idea but modifying the election procedure.

The first step in our approach is to choose the cluster-heads that will ensure the protection of their respective cluster. Indeed, a cluster-head supports the monitoring of its cluster members traffic. In other words, when a packet is directed to one node, the cluster-head intercepts it, tests it and retransmits it to its destination if the packet is not a threat.

Clustering algorithm

Gerla and Tsai proposed in [12] a clustering algorithm, called High-Connectivity Clustering (HCC), where the election of cluster-heads is based on the higher degree criteria. The node's degree is calculated as a function of its distance from the others. The different steps of this algorithm are as follows:

(1) *Each node broadcasts its ID to the nodes that are in its transmission range (its neighbors) and the node with a maximum number of neighbors, i.e. with a maximum degree, is chosen as a cluster-head and its neighbors become members of this cluster and can't participate in the following election process.*
(2) *The process continues until there are no more nodes to affiliate to the cluster.*

The advantage of this algorithm is that it generates a reduced number of cluster-heads and provides a low rate cluster-head changes, but it does not take into consideration the energy constraint which is an important factor for the network. For this, we added a preliminary phase that takes into account the energy level of nodes in the election procedure of cluster-head. The proposed clustering algorithm takes the following form:

Proposed algorithm

(0). Initialization: Initialization step consists on:
- Assign to each node an initial position and fix its initial load energy. In this work, the initial nodes positions are random and all the nodes have the same initial load energy. But it is very easy to consider the initial load energy is also random.
- Fix the required energy threshold for a node to be in priority in the election process of the cluster-head. In *Ad hoc* networks, most of the energy are wasted in retransmission [13], for this reason, define an energy threshold for a cluster-head ensures the improvement of the network lifetime and reduces the problem of immediately link brakeage.

(1). Calculating degree: Calculate the degree of each node which corresponds to the number of its neighbors at 1-hop;

(2). Energy test: This step consists on selecting a set S, which contains the nodes satisfying the threshold fixed in the initialization step;

(3). Selection of cluster-heads: In this stage, the set S can be empty or contains at least a single element:
- **If** $S \neq \emptyset$:

(3.1) The principle of HCC algorithm will be applied: select the node of highest degree in the set S, that will be noted CH,

(3.2) S=S\{CH};
- **Else** (S = ∅): Apply the HCC algorithm on the set of the remaining nodes;

(4). Attachment to the cluster-heads: Once the cluster-head is elected, all its neighbors at 1-hop join him and they form a cluster.

Steps (3) and (4) are repeated until all nodes are affiliated to the clusters either as a cluster-head or a member.

Since *Ad hoc* network nodes are dynamic with limited energy, it would be indispensable to update the clustering procedure. Thus, each node is potentially able to be elected as cluster-head. It is therefore necessary to install IDS on all nodes of the network and keep them on standby until they are elected as cluster-heads.

2.2. Evolutionary game

In this second step, we propose a game model describing the strategic behavior of cluster-heads in evolutionary game form. In [16], the authors considered that the population is constituted of all network nodes, while in our approach we limit ourselves only to cluster-heads. On the other hand, unlike [16], in the definition of players utility, we consider the damage and loss caused in the case where the network is not secure. Once the network is partitioned into clusters and the cluster-heads are elected, we consider the game between the cluster-heads. Each cluster-head has two pure strategies:

(1) Protect (P), which results by activating of its IDS.
(2) Not Protect (NP) by deactivating its IDS.

A cluster-head, which contributes to his cluster security in choosing the strategy (P), supports a cost c corresponding to the energy expenditure when it ensures the safety of its cluster when activating its IDS. In this case, the cluster-head obtains a reward r for the safety of its cluster which coincides to the preservation of confidentiality, integrity and availability of its data. When a cluster-head chooses not to activate its IDS, it becomes not safe as well as its cluster members, because they are supposed to be constantly exposed to attacks. So, loss of security when the attacks are successful can generate the loss of reputation or data integrity. The cost of damage control will be denoted l. In practice, the security assets are evaluated in the risk analysis/assessment phase using formal analysis or specific tools before the IDS deployment [9].

The cluster-heads choose simultaneously their strategies. The players' utilities are based on the following observations:

- If the both players choose to protect and active their IDS, each of the two-players receives the reward r which will be reduced by the activation cost c.
- In the case where only one of them chooses to active its IDS, the cluster-head who chooses to protect will pay cost of damage control, furthermore, it will also have to spend a cost corresponding to the activation of its IDS, thus its utility is $(-c-l)$, and one who does not activate its IDS, will have to pay only cost of damage control $(-l)$.
- In the last case, where no one of the players chooses to protect, their safety will be compromised and both have losses equivalent to l.

Thus, the game between two cluster-heads can be represented in strategic form, Table 1 below where: r, c and $l > 0$.

In order to encourage the cluster-heads to activate their IDS, we suppose

$$r > c \text{ and } l > c. \tag{2.1}$$

As the considered game is symmetric, we consider only one payoff matrix

$$A = \begin{matrix} \\ P \\ NP \end{matrix} \begin{matrix} \begin{matrix} P & \quad NP \end{matrix} \\ \begin{pmatrix} r-c & -c-l \\ -l & -l \end{pmatrix} \end{matrix}. \tag{2.2}$$

TABLE 1. Strategic form.

	P	NP
P	$(r-c, r-c)$	$(-c-l, -l)$
NP	$(-l, -c-l)$	$(-l, -l)$

A Pareto efficient equilibrium is a state in which it is no longer possible to improve the gain of a player without decreasing that of another. Therefore, the equilibrium (P, P), the two players choose to activate their IDS, is Pareto efficient giving both players a reward equivalent to $(r-c)$. The other equilibrium (NP, NP) is less efficient, no cluster-head contributes to the security of the network, which generates for each one a loss l.

Let u_1 the utility function of player 1. The *resistance* [16,18] of the equilibrium (NP, NP) against equilibrium (P, P) is the largest number $\alpha \in [0, 1]$ such that:

$$\begin{aligned} \alpha u_1(NP,P) + (1-\alpha)u_1(NP,NP) &\geq \alpha u_1(P,P) + (1-\alpha)u_1(P,NP) \\ \Rightarrow \alpha(-l) + (1-\alpha)(-l) &\geq \alpha(r-c) + (1-\alpha)(-c-l) \\ \Rightarrow -\alpha(r+l) &\geq -c \\ \Rightarrow \alpha &\leq \frac{c}{r+l} \end{aligned}$$

The *resistance* of equilibrium (NP, NP) against (P, P) is $\alpha = \frac{c}{r+l}$. Thus, the *resistance* of equilibrium (P, P) against (NP, NP) is 1 - $\alpha = \frac{r+l-c}{r+l}$.

The equilibrium (NP, NP) *risk dominates* the equilibrium (P, P) if and only if the *resistance* of (NP, NP) against (P, P) is greater than the *resistance* of (P, P) against (NP, NP). *i.e.*, if $\alpha > 1-\alpha \Rightarrow \frac{c}{r+l} > \frac{1}{2}$. Thus, $\frac{c}{r+l}$ is called the *risk factor* for the equilibrium (P, P) [16].

The considered game is symmetrical, so, the results of the second player are the same as those obtained above.

In evolutionary games, the probability α that the strategy P is selected corresponds to the initial proportion of the population choosing the strategy P. Hence, according to the resistance calculation, we deduce that for initial proportions of the population less than $\frac{c}{r+l}$, the (NP,NP) equilibrium provides a better gain than the (P,P) equilibrium. This implies an increasing of the population proportion which chooses the NP strategy.

The evolutionary games allow to model the dynamic evolution of a population of interacting individuals using two fundamental concepts: the evolutionary stable strategy (ESS) and the replicator dynamic.

Definition 2.1. [17] A strategy $p \in \Delta$ is an evolutionary stable strategy (ESS), if: $\forall q \in \Delta, \exists\ \bar{\varepsilon} = \bar{\varepsilon}(q) \in (0,1), \forall \varepsilon \in (0, \bar{\varepsilon})$,

$$u(p, (1-\varepsilon)p + \varepsilon q) > u(q, (1-\varepsilon)p + \varepsilon q), \tag{2.3}$$

where Δ is the set mixed strategies of a player.

Proposition 2.2.

(1) *$p \in \Delta$ is an ESS $\Rightarrow$ p is a Nash equilibrium;*
(2) *$p \in \Delta$ is a strict Nash equilibrium $\Rightarrow$ p is an ESS.*

The matrix game (2.2) admits two strict Nash equilibria: (P,P) and (NP,NP), and thus, according to the Proposition 2.2, the corresponding evolutionary game admits two ESS.

The matrix game (2.2) admits a Nash equilibrium in mixed strategies (p^*, q^*), with $p^* = q^* = (\frac{c}{r+l}, \frac{r+l-c}{r+l})$. In adopting this strategy, each cluster-head plays P with probability $\frac{c}{r+l}$.

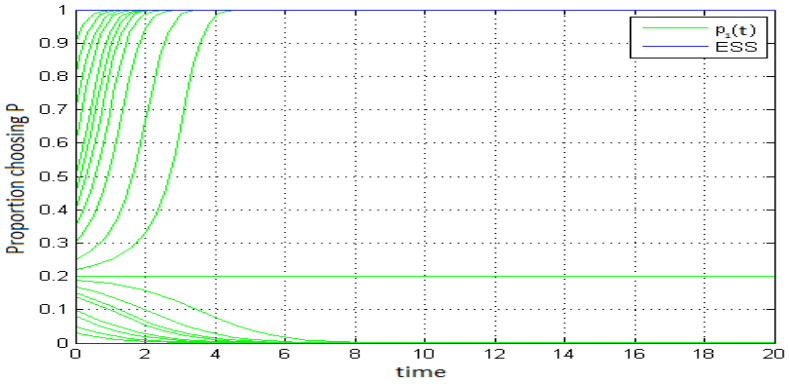

FIGURE 1. Convergence of replicator dynamic.

2.3. Replicator dynamic

The replicator dynamic is selection process specifying how a population is associated with various pure strategies in a game which evolves in time, it is governed by the following system of differential equations [14]:

$$\dot{p_i} = p_i[(Ap)_i \ - \ p^T Ap], \qquad i = 1, 2. \tag{2.4}$$

With the payoff matrix (2.2), the system (2.4) takes the following form:

$$\dot{p_1} = p_1(1 - p_1)[p_1(l + r) - c] \ \ , \ \ \dot{p_2} = -\dot{p_1},$$

where p_1 is the proportion of population playing the strategy (P) and p_2 the proportion of population playing the strategy (NP).

In order to study the evolution of population, we implemented the replicator dynamic, with game parameters: $r = 3$, $c = 1$ et $l = 2$. Figure 1 illustrates results for different initial proportion of population that choose the strategy (P). The proportion is varying between 0 and 1.

We remark from the Figure 1 that:

- With initial rate of population choosing a strategy (P) strictly less than $0.2 = \frac{c}{r+l}$, the number of cluster-heads which participate for security decreases until all cluster-heads decide not to participate.
- With initial rate of population choosing a strategy (P) strictly greater than 0.2, the number of cluster-heads which participate for security increases until all cluster-heads decide to participate.
- With initial rate of population choosing a strategy (P) equal to 0.2, the number of cluster-heads which participate for security remains the same.

Thus, the results that give us the implementation of the replicator dynamic, validate the theoretical results obtained in Section 2.2.

3. MAIN ALGORITHM

Here, we give a general description of our approach, integrating the energy constraint for the cluster-heads election procedure and the evolutionary game to determine the cluster-heads proportion who activate their IDS.

(1) **Initialization**

(a) Insert the r safety benefit, the IDS activation cost c and cost of damage control l.

TABLE 2. Simulation parameters.

(X, Y)	1000 m × 1000 m
N	20
R	250 m
$[v_{min}, v_{max}]$	[0, 15]
Mobility Model	Random Walk
$Einitial$	100 J
$Threshold$	25 J
T	150 s
h	15 s

(b) Insert the initial participation rate, energy level of each node, the energy threshold, nodes positions , speeds, and other network parameters.

(2) **Clustering**
Apply the clustering algorithm presented in Section 2.1 and get the list of clusters-heads.

(3) **The game**
Set up the game and the replicator dynamic is used to obtain the cluster-heads proportion who must participate in security by enabling their IDS;

(4) **Update**
Update the energy level of nodes.
If there are at least one node with a positif energy level then calculate the new positions of active nodes, go to step (2);
Else **End**.

4. SIMULATION

In this section, we evaluate the performances of our approach in two steps: clustering-evolutionary game.

4.1. Simulation parameters

The implemented *Ad hoc* network is defined by its area[3] and the number of nodes that it contains. The area of network is 1000 m × 1000 m containing $N = 20$ nodes. Initially, we assign $Einitial = 100$ J to each node which decreases with quantity equal to 10 J [7] in the case of activation of the IDS, and with randomly quantity selected in the interval [5 J, 15 J] during a reception or transmission of packets. The mobility model is the Random Walk with speed $v \in [0, 15$ m/s] and a movement direction $\theta \in [0, 2\pi]$. We set the transmission range of each node to $R = 250$ m.

The simulation time is $T = 150$ s. The nodes change position every $h = 15$ s with different directions and speeds. For a node, the necessary threshold to become priority for being cluster-head is $Threshold = 25$ J. Table 2 summarizes our simulation parameters:

4.2. Simulation results

The simulation which lasts 150 s, was made according to the parameters listed in Table 2. The graphical representation of the last positions of nodes is shown in Figure 2 below.

[3]Size in X and Y coordinates.

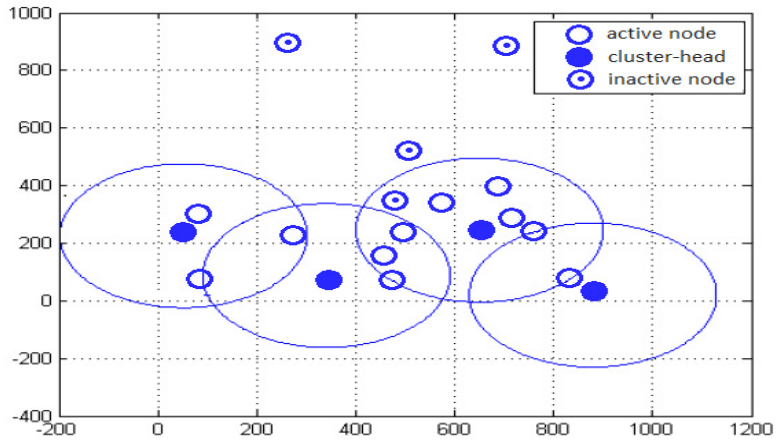

FIGURE 2. Nodes positions.

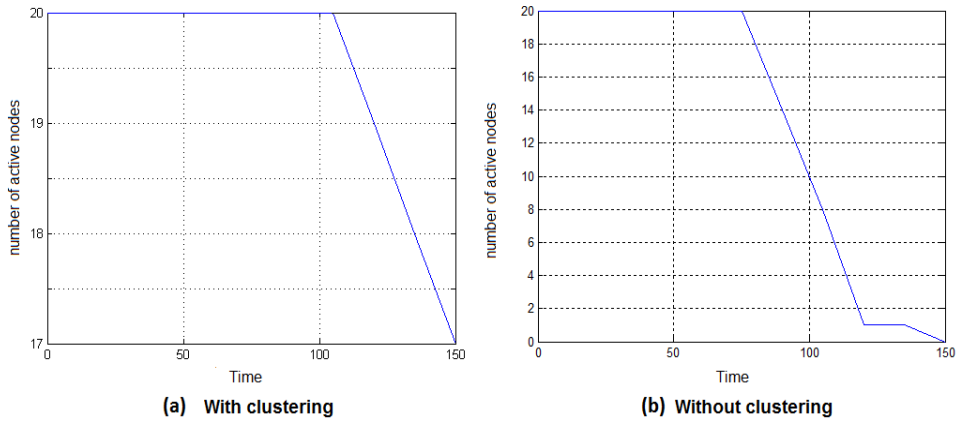

FIGURE 3. Evolution in the time of the number of active nodes.

The inactive nodes[4] may be considered as isolated nodes[5] although they are geographically in one cluster or more, because they are invisible to other nodes and can't maintain network connectivity.

4.3. Clustering evaluation

The aim of clustering is to manage better energy consumption of nodes while keeping up the security of the network by activating only the IDS of cluster-heads. We made a comparative study between the approach we developed in this paper (step with clustering) and an approach that does not use this step (step without clustering). The comparison of these two approaches is based on the following criteria: the average number of inactive nodes and the average number of isolated nodes.

For the same simulation parameters, we will represent the number of active nodes according to time for the two models, with clustering and without clustering, see Figure 3.

[4]An inactive node is a node whose energy is equal to 0.

[5]An isolated node is a node whose set of 1-hop neighbors is empty.

TABLE 3. Comparison between two approaches with/without clustering for different values of N and T.

	1st instant where the 1st node becomes inactive		Number of nodes still active at T	
	With clustering	Without clustering	With clustering	Without clustering
$T = 300$, $N = 150$	200	53	141	0
$T = 250$, $N = 300$	243	60	298	0
$T = 1000$, $N = 500$	240	50	0	0

TABLE 4. Connectivity of the network.

		With clustering	Without clustering
$N = 20$, $T = 150$	Mean number of isolated nodes	9	20
	Mean probability of connectivity	0.4	0
$N = 300$, $T = 250$	Mean number of isolated nodes	2	300
	Mean probability of connectivity	0.99	0

From Figure 3, we remark:

- The moments when the first node becomes inactive for the two models, with clustering and without clustering, are respectively 120 and 80 s;
- The number of active nodes in the model without clustering rapidly decreases until it becomes 0 at the end of the simulation. In contrast, the number of active nodes in the model with clustering decreases slowly and at the end of the simulation we find only three inactive nodes.

By making other simulations with a larger number of nodes and different simulation times, we obtain the Table 3.

According to Table 3, we note that the increasing of the number of nodes and simulation time give as good results as in the case where the number of nodes is only 20. This shows further the clustering effectiveness in energy conservation, which allows for nodes to remain active longer and hence to participate more in the network security mechanism.

In sum, the results concerning the number of active nodes given by the model with clustering are significantly better than those obtained by the model without clustering. This difference clearly shows how the clustering and activation of IDS only on cluster-heads affect the number of active nodes in a network.

The average number of isolated nodes and the average probability of connectivity of the network during the simulation are given in Table 4.

We see from the Table 4 that a clustered network is more connected than a non-clustered network. Indeed, in a clustered network, the energy of nodes decreases more slowly compared to a non-clustered network because the activation of the IDS is only made by the cluster-heads. Therefore, the number of inactive nodes in a clustered network is increasing slowly. Thus, the network remains connected for long time. So, we can say that the clustering maintains the network connectivity.

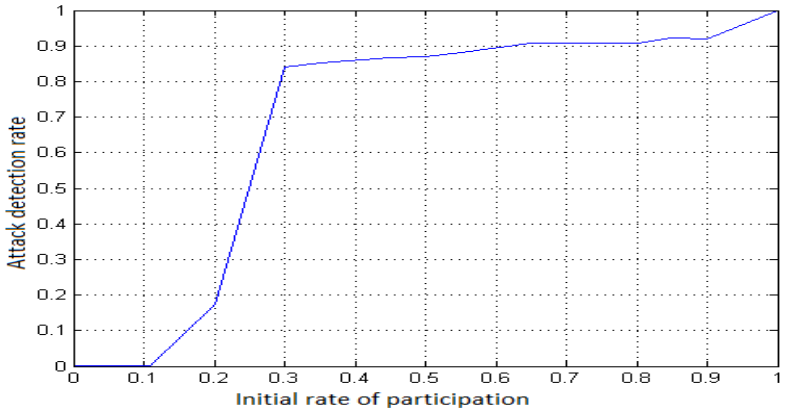

FIGURE 4. The impact of the initial rate of participation to the security on attacks detection rate.

4.4. Impact of the initial rate of participation to the security on the attacks detection rate

During the simulation, we generated attacks, and in order to observe the impact of the initial rate of participation to the security on the detection rate of these attacks, we have implemented the dynamic replicator in the simulator. Thus, given the set of cluster-heads which chose the strategy (P) and the set of nodes attacked, we could obtain the detection rate at each attacks generation. We consider the game parameters: $r = 3$, $l = 2$ et $c = 1$, the evolution of rate detection as a function of the initial rate of participation is illustrated in the Figure 4:

According to Figure 4, we notice that:

- For initial rates lower than 0.2 ($p_1(0) < 0.2$), the detection rate is not very important because the cluster-heads end up not to participate and therefore all attacks generated from this moment will not be detected.
- When the initial rates surpass 0.2 ($p_1(0) > 0.2$), the associated rates of detection are high because such states always end up reaching the evolutionary stable strategy $p_1^* = 1$ which means that all cluster-heads choose to participate and all the attacks generated will be detected.

4.5. Comparative study

Figure 5 represents a comparison between HCC and our proposed algorithm (HCC-Energy) in term of network lifetime. According to the simulation results, we see that with basic HCC there are 30% more inactive nodes than in the HCC-energy algorithm that we have proposed which take into account energy and promotes the election of nodes whose residual energy is above the threshold.

The HCC-energy algorithm allows to not fully exhaust the energy resources of the nodes and thus the network remains more connected and more secure.

Unlike to our game model, the one proposed in [16] does not take into account the security losses caused when the cluster-heads choose not protect (NP) and consequently the authors set $l = 0$. In order to highlight the impact of the security losses on the population evolution, we will make a comparison between our replicator dynamic which considers $l = 2$ and the replicator dynamic associated to the case $l = 0$. Figure 6 shows the implementation of the two replicators dynamic.

From Figure 6, we notice that:

- In our model, $l > 0$, the required initial proportion for that all the cluster-heads end up participating in security is $\frac{c}{r+l} = 0.2$ and it is small than $\frac{c}{r} = \frac{1}{3}$ which corresponds to the case when $l = 0$.

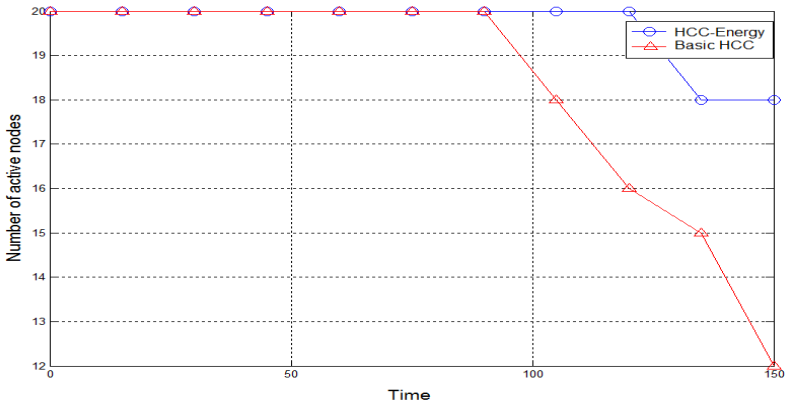

FIGURE 5. Lifetime comparison.

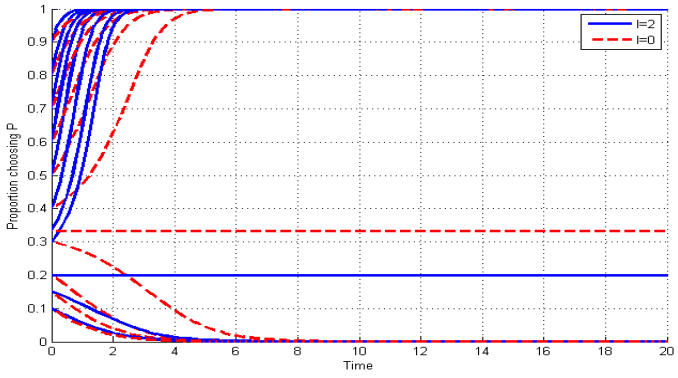

FIGURE 6. Replicator dynamic comparison.

- For the same initial rates, the replicator dynamic associated to our model, $l > 0$, converges faster towards 1, so all the cluster-heads end up participate in security more quickly when we assume losses ($l > 0$) than when $l = 0$. For example, with an initial proportion $p_1(0) = 0.4$, all cluster-heads activate their IDS at time $t = 2$ in our model and at time $t = 5.2$ in the model proposed in [16]. So, our proposal encourages more cluster-heads to participate to the network security.
  In the other hand, when the replicator dynamic converges to 0, this happens less quickly when we put $l > 0$. In conclusion, putting $l > 0$, cluster-heads are effectively incited to participate in the security.

5. CONCLUSION

In this work, we have treated the problem of security in *Ad hoc* networks by a two-steps approach: clustering and modeling by evolutionary game. We have optimized the utilization of nodes energy resources through a clustering. We also highlighted the evolutionary aspect of the network to monitor the interactions between the cluster-heads of the network in their participation in security process.

We have identified the convergence conditions of the replicator dynamic, which describes the evolution of cluster-heads population playing strategy (P), to the ESS. These conditions were confirmed in the implementation of the replicator dynamic. The integration of the replicator dynamic in the simulator allowed us to see that

the detection rate is an increasing function of the initial population rate playing (P). The comparison between our model and a without-clustering model enabled us to confirm that the clustering technique is effective for reducing the number of inactive nodes, therefore the number of isolated nodes, which makes the network more connected while maintaining its security.

Our simulations also showed that introducing an energy criterion in the cluster-heads selection in our clustering algorithm would distribute more evenly the energy expenditure among the network nodes and improves the network lifetime.

The replicator dynamic implementation results show that introducing a cost for a cluster-head that does not activate its IDS, encourages more cluster-heads to participate to the network security.

As an outlook, we can use a more realistic energy consumption model, which distinguishes between the energy consumed during transmission and the energy consumed when receiving a message.

Acknowledgements. The authors are grateful to the anonymous referees for their remarks and comments which have helped to improve and clarify the paper.

References

[1] K. Adel-Aissanou, D. Aïssani, N. Djellab and N. Mikou, A stochastic model to study the impact of the transmission frequency of hello messages on the connectivity of Ad hoc Networks. *Telecommun. Syst.* **57** (2014) 197–207.

[2] R. Agarwal and M. Motwani, Survey of Clustering Algorithms for MANET. *Int. J. Comput. Sci. Eng.* **2** (2009) 98–104.

[3] L. Aliahmadipour and M.M. Javidi, Game Theory Approaches for Improving Intrusion Detection in MANETs. *Sci. Res. Essays* **31** (2011) 6535–6539.

[4] T. Alpcan, T. Başar and K.C. Nguyen, Stochastic Games for Security in Networks with Interdependent Nodes. *Proc. of Int. Conf. Game Theory Networks, GameNets* (2009).

[5] D.J. Baker, A. Ephremides and J.E. Wieselthier, A Design Concept for Reliable Mobile Radio Networks with Frequency Hopping Signaling, In *Proc. of the IEEE* **75** (1987) 56–73.

[6] C. Bettstetter, On the connectivity of Ad Hoc Networks. *Comput. J.* **47** (2004) 442–447.

[7] P. Bhattacharya, M. Debbabi, N.Mohammed, H. Otrok and L. Wang, Mechanism design-based secure leader election model for intrusion detection in MANET. *IEEE Trans. Dependable Secure Comput.* **8** (2011) 89–103.

[8] M. Chatterjee, S. K. Das and D. Turgut, WCA: A weighted clustering algorithm for mobile Ad Hoc Networks. *Clust. Comput.* **5** (2002) 193–204.

[9] L. Chen and J. Leneutre, A game theoretical framework on intrusion detection in heterogeneous networks. *Trans. Inf. Fotrnsics Security* **4** (2009) 155–178.

[10] C. Comaniciu, Y. Liu and H. Man, A Bayesian Game Approach for Intrusion Detection in Wireless Ad Hoc Networks. *Proc. of GameNets (Workshop on Game Theory for Networks)*, Pise, Italie (2006) 1–12.

[11] S. Fahmy and O. Younis, HEED: A hybrid energy-efficient distributed clustering approach for Ad Hoc sensor networks. *IEEE Trans. Mobile Comput.* **3** (2004) 366–371.

[12] M. Gerla and J. Tzu-Chieh Tsai, Multicluster mobile, multimedia radio network. *ACM/Baltzer J. Wireless Networks* **1** (1995) 225–265.

[13] R. Jain and S. Dewivedi Sharma, A Novel Energy threshold based Location Aided Routing in MANET, *Int. J. Comput. Sci. Inform. Technol.* **4** (2013) 392–397.

[14] L.B. Jonker and P. D. Taylor, Evolutionary stable strategies and game dynamics. *Math. Biosci.* **40** (1978) 145–156.

[15] R. Kalaivani and D. Ramya Dorai, Cluster based leader election and intrusion detection system for MANET. *Int. J. Comput. Sci. Manag. Res.* **2** (2013) 1459–1462.

[16] C.A. Kamhoua, K. makki and n. pissinou, game theoretic modeling and evolution of trust in autonomous multi-hop networks application to network security and privacy. *IEEE Commun. Soc.* (2011) 1–6.

[17] J. Maynard Smith and G.R. Price, The logic of animal conflict. *Nature* **246** (5427) 15–18 (1973).

[18] R. Myerson, Game Theory: Analysis of Conflict. Harvard University Press (1997).

[19] E.A. Panaousis and C. Politis, Non-Cooperative Games Between Legitimate Nodes and Malicious Coalitions in MANET's. *Proc. of the Future Network and Mobile Summit 2011 conference* (2011).

[20] A.C. Santos, C. Duhamel, L.S. Belisario and L.M. Gueds, Strategies for designing energy efficient clusters-based WSN topologies. *J. Heuristics* **18** (2012) 655-675.

[21] H. Sun and H. Wei, Using Bayesian Game model for intrusion detection in wireless Ad Hoc Networks. *Int. J. Commun., Network Syst. Sci.* **3** (2010) 602–607.

[22] K. Wei Lye and J.-M. Wing, Game strategies in network security. *Int. J. Inform. Security* **4** (2005) 71–86.