Future Network and MobileSummit 2011 Conference Proceedings
Paul Cunningham and Miriam Cunningham (Eds)
IIMC International Information Management Corporation, 2011
ISBN: 978-1-905824-23-6

Poster Paper

Non-Cooperative Games Between Legitimate Nodes and Malicious Coalitions in MANETs

Emmanouil A. PANAOUSIS and Christos POLITIS
Wireless Multimedia & Networking (WMN) Research Group
Kingston University London, UK
Tel: +442084172653, Email: {e.panaousis,c.politis}@kingston.ac.uk

Abstract: Security for mobile ad hoc networks (MANETs) is a critical and thoroughly examined scientific area that has attracted the interest of many researchers. Many countermeasures against compromised or selfish nodes consider intrusion detection systems (IDS). In this paper we use game theory to model non-cooperative security games between a MANET, which is defended by IDS operating at each node as well as a group of collaborative malicious nodes called *malicious coalition*. Our work innovates by finding the defend and attack probability distributions, of any MANET and malicious coalition, that maximise the utility of the players at the Nash Equilibrium (NE) of a non-cooperative security game between the aforementioned entities. To go a step further, this paper proposes a way to derive the intrusion detection or the attack effort respecting the corresponding energy costs of the MANET and the malicious coalition. Parameters such as intrusion detection rate, attacking cost, defending cost, false alarm detection rate and false alarm cost critically affect the final defending and attacking distribution probabilities as we have shown in this paper. Numerical results have been illustrated showing the changes at MANET's utility, at NE, as a function of the packet size, the intrusion detection rate and the mobility.

Keywords: MANET, game theory, intrusion detection, security

1. Introduction

Mobile ad-hoc networks (MANETs) have attracted the interest of several scientists due to their easy employability in case communication has to be established in a decentralised manner. A paradigm where MANETs are really useful to be deployed might be an emergency case where rescuers have to coordinate their actions [1]. In contrast to wired networks, which have a higher level of security for gateways and routers, MANETs have characteristics that make them more susceptible to attacks. For instance due to MANETs' wireless nature, prospective attacks can be launched by anyone and from any direction. Jamming constitutes a paradigm of such an attack which can totally damage a MANET. Furthermore, the MANET nodes must cooperate with each other to accomplish specific goals and thus selfish behaviour can introduce several problems such as a node might drop legitimate packets launching a blackhole (Denial of Service) attack.

MANET security is usually based on encryption and authentication techniques. However, such schemes are not always sufficient due to insider attacks launched by compromised or captured nodes. Since such risks cannot be completely eliminated there comes a need for intrusion detection systems (IDS) to defend MANETs ([2], [3]). IDS can constitute a second wall of defence and their role is critical since the majority of MANETs will be deployed in hostile environments in which legitimate nodes can be captured and

operated by adversaries (i.e. node capture attacks). Nodes that are equipped with IDS sensors, operating in promiscuous mode, can monitor the traffic sent or received by their neighbours in order to detect malicious activities or deviation from conventional behaviours.

In this paper we use game theory to model non-cooperative security games between a MANET, which is defended by IDS sensors operating at each node, and a group of collaborative malicious nodes called *malicious coalition*. Our work innovates by finding the defend and attack probability distributions, of any MANET and malicious coalition, that maximise the utility of the players at the Nash Equilibrium (NE) of a non-cooperative security game between the aforementioned entities. These probability distributions represent the percentage of the computational effort spent for defending or attacking the nodes of a MANET. In other words, this paper proposes a way to derive the intrusion detection or the attack "effort" that a MANET or a malicious coalition, correspondingly, have to give in respect with their energy costs. Parameters such as intrusion detection rate, attacking cost, defending cost, false alarm detection rate and false alarm cost critically affect the final defending and attacking distribution probabilities as we have shown in this paper.

The remainder of this paper is structured as follows. In section 2 we discuss related work within the realm of MANET security with game theoretic considerations. In section 3 we describe our system model defining the different our game parameters and the utility functions of each player. In section 4 we have derived the NE of the security game whilst section 5 shows some numerical results about the utility of the MANET for different packet sizes, MANET types, mobility levels, and intrusion detection capabilities. We finally conclude this paper in section 6 summarising the main findings and mentioning our plans for future work.

2. Related Work

Few works propose game theoretic solutions for intrusion detection or security provision within the realm of MANETs. The most important of them, according to our opinion are the [4], [5], [6], [7], [8], [9], [10] and [11]. To the best of our knowledge none of them propose a method of calculating the defending and attacking probability distributions over a MANET's nodes by maximising the utility of the MANET and any malicious coalition at the NE.

In the paper [4] authors have modelled the interactions between a host-based IDS and an attacker as a basic signalling game which can be seen as a dynamic non-cooperative game with incomplete information. The authors have not however considered colluding attackers or any malicious coalition. In addition, the [5] proposes a distributed mechanism which extends the lifetime of a cluster IDS model by electing different IDS leaders each time. The paper proposes a cooperative game model to catch the misbehaving IDS leaders whilst minimising the false positive rate. On the other hand, a zero-sum non-cooperative game model has been proposed in order to maximise the probability detection done by the leader-IDS. The model helps the leader-IDS to use its optimal sampling strategy when intrusion detection takes place. In [6], we have proposed a game theoretic approach called AODV-GT (Game Theoretic) and we integrated it into the AODV protocol. According to AODV-GT, each node chooses to route its packets through the route, which satisfies the following criteria; (i) less number of

black hole nodes probabilistically attack this route, (ii) less energy consumption of the participated Host-IDS. These criteria maximise the utility of the MANET at the NE.

In [8] authors have proposed a Bayesian game formulation to support intrusion detection in wireless ad hoc networks. According to this paper the defender tries to maximise his defending capabilities with respect in his energy cost while the attacker tries to damage the network without being detected. The authors have considered both static and dynamic games. For the static game they have derived the mixed-strategy Bayesian NE (BNE) and the pure-strategy BNE. They have additionally derived the mixed-strategy Perfect Bayesian Equilibrium (PBE) of the dynamic game proposing at the end a hybrid detection approach which uses the dynamic game model to compute equilibrium strategies for the players.

In [9] authors use a dynamic Bayesian game framework to analyse the situation between regular and malicious nodes in a MANET. A regular node selects the probability to cooperate with its opponent based on the belief it has about the others and he rationally decides to report misbehaviours. On the other hand, a malicious node estimates the loss if it gets caught and when required it tries to flee in order to avoid punishment. By analysing the PBE of the game the authors show the attackers' profit when they decide to flee. They however do not consider any malicious coalition but they examine only the regular/malicious node game.

Authors in [7] exploit ways to to enforce cooperation in autonomous ad hoc networks when conditions of noisy and imperfect observation happen. They actually model the packet forwarding as a repeated game with imperfect information and they have developed a framework to enforce cooperative packet forwarding even in presence of noisy channels. They have also proven that the behavioural strategy refines the NE point and it offers high payoffs. The same authors in [11] they have examined the dynamic interactions between good nodes and adversaries in MANETs as secure routing and packet forwarding games. They have derived optimal defense strategies whilst the maximum potential damaged which could be caused by attackers has been studied.

In [10] authors have used a game theoretic framework to examine secure cooperation stimulation in autonomous MANETs. Selfish and malicious possible behaviours have been studied whilst incentives are given to stimulate attack-resistant cooperation even under noisy and hostile networks. In terms of game theory, the authors study a two-player packet forwarding game. Towards the decision of good cooperation strategies, they have refine the NE solutions considering aspects such as subgame perfection, fairness, Pareto optimality and cheat-proofing. They conclude at a unique NE in which none of the MANET nodes has to help it opponent than the latter has helped it.

3. System Model

A solution of a two-player game is a pair of strategies that a rational pair of players might use. The solution that is most widely used for game theoretic problems is the Nash equilibrium (NE) [12]. At a NE, given the strategies of other players, no user can improve its utility level by making individual changes in its strategy. In maths terms, let $\mathcal{G} = (\mathcal{S}, \mathcal{U})$ be a game, where $\mathcal{S}$ is the set of strategy profiles and $\mathcal{U}$ is the set of payoff profiles. Let s_{-i} be a strategy profile of all players except for player i. When each player $i \in \{1, ..., n\}$ chooses the strategy s_i resulting in the strategy profile $s = (s_1, ..., s_n)$ then the player i obtains payoff or utility equal to $u_i(s)$. The utility depends on the strategy

chosen by player i as well as the strategies chosen by all the other players. A NE in a n-player game is a list of mixed strategies $s_1^*, ..., s_n^*$ such that:

$$s_i \in arg\max_{s_i \in S_i} u_i(s_i, s_{-i}) \ \forall \ i \in \{1, 2, ..., n\} \tag{1}$$

In other words according to [13]:

Lemma 1 *A strategy profile $s^* \in S^*$ is a NE if no unilateral deviation in strategy by any single player is profitable or; $\forall\ i,\ u_i(s_i^*, s_{-i}^*) \geq u_i(s_i, s_{-i}^*)$.*

In our work we have assumed that nodes are equipped with intrusion detection sensors. Once the data are collected by the IDS sensors, they are analysed to detect malicious activities. Upon detection, punishment strategies are applied to defend MANET against the attacks.

In the examined cases the IDS coexist with malicious entities in a MANET. Consequently, a security game $\mathcal{G}_{\mathcal{SG}}$[1] is emerging between the IDS and one or more adversaries. From now on, we will consider all the attackers as one player called *malicious coalition* and all the IDS as one player, the *MANET*. We define the game's strategy space as $\mathcal{S}_{\mathcal{SG}} = \{(d,\ a),\ (d,\ na),\ (nd,\ a), (nd,\ na)\}$, where d denotes defending, a: attacking, nd: non defending, and na: non attacking whilst the utility space equals to $\mathcal{U}_{\mathcal{SG}} = \{U_{manet}, U_{mc}\}$.

Goal of the malicious coalition is to attack the MANET without being detected whereas that of the MANET is to recognise any malicious behaviour. Since there is no cooperation between the two players, the discussed game is characterised as non-cooperative. When an attack is indeed in progress one of the following cases may occur: (i) the MANET has not detected the attack due to IDS limitations. This might happen for instance in cases where the IDS software has not been updated with a known or a new attack or the IDS capabilities are limited, (ii) the MANET has not recognised the attack due to malfunction, (iii) the MANET has recognized the attack and triggers an alarm.

In all the above cases the mis-detection rate equals to $1 - r_d$ where r_d is the attack detection rate. On the other hand, when there is no attack in progress the MANET might produce a false alarm due to malfunctioning or the attack detection mechanism has falsely concluded that an attack was in progress.

We define $\mathbf{P_d} = (p_{d,1},\ p_{d,2},\ ...,\ p_{d,n})$ as the defend probability distribution over $\mathcal{N}$ and $\mathbf{P_a} = (p_{a,1},\ p_{a,2},\ ...,\ p_{a,n})$ as the attack probability distribution over $\mathcal{N}$. These satisfy the following constraints: $\sum_{n \in \mathcal{N}} p_{d,n} \leq P_d$ and $\sum_{n \in \mathcal{N}} p_{a,n} \leq P_a$. Assuming the different parameters $0 < r_d,\ r_f,\ cost_a,\ cost_d,\ cost_f \leq 1$, where r_f is the false alarm rate, $cost_a$ is the attacking cost, $cost_d$ is the intrusion detection cost, $cost_f$ is the cost due to a false alarm (i.e. cost spent to react[2] due to a falsely detected attack).

In Table 1 we show the utility functions of the MANET and the malicious coalition for the different strategy tuples; $0 < V_{n_i} \leq 1$ indicates the loss of security when an attack against a node $n_i \in \mathcal{N}$ is successful. For simplicity reasons we assume that $V_{n_i} = V_{n_j} = V,\ \forall\ i, j \in\ \mathcal{N}$. It is worth mentioning that since the attacker aims at gaining some utility he expects that $cost_a < V$ otherwise he is not motivated to attack

[1] it stands for Security Game (SG)

[2] enabling a punishment strategy

Table 1: Security Game's Payoff Matrix

strategy	*Attacking*	*Non Attacking*
Defending	$-(1-r_d)V_{n_i} - r_f cost_f V_{n_i} - cost_d V_{n_i}$, $(1-r_d)V_{n_i} - cost_a V_{n_i}$	$-r_f cost_f V_{n_i} - cost_d V_{n_i}$, 0
Non Defending	$-V_{n_i}$, $V_{n_i} - cost_a V_{n_i}$	0, 0

any node. The overall utility functions for both players are given by the following equations:

$$\begin{aligned} U_{manet}(P_d, P_a) &= \sum_{n_i \in N} p_{d,n_i} p_{a,n_i} [-(1-r_d)V_{n_i} - r_f cost_f V_{n_i} - cost_d V_{n_i}] \\ &+ \sum_{n_i \in \mathcal{N}} p_{d,n_i}(1-p_{a,n_i})(-r_f cost_f V_{n_i} - cost_d V_{n_i}) + \sum_{n_i \in \mathcal{N}} (1-p_{d,n_i}) p_{a,n_i}(-V_{n_i}) \\ &= \sum_{n_i \in \mathcal{N}} V_{n_i} [p_{d,n_i}(r_d p_{a,n_i} - r_f cost_f - cost_d) - p_{a,n_i}] \end{aligned} \tag{2}$$

$$\begin{aligned} U_{mc}(P_d, P_a) &= \sum_{n_i \in \mathcal{N}} p_{a,n_i} p_{d,n_i} [(1-r_d)V_{n_i} - cost_a V_{n_i}] + \sum_{n_i \in \mathcal{N}} p_{a,n_i}(1-p_{d,n_i}) V_{n_i}(1-cost_a) \\ &= \sum_{n_i \in \mathcal{N}} V_{n_i} p_{a,n_i}(-p_{d,n_i} r_d + 1 - cost_a) \end{aligned} \tag{3}$$

Before we derive the NE solution of the $\mathcal{U}_{\mathcal{SG}}$, $(\mathbf{P_d^*}, \mathbf{P_a^*})$, we must verify the existence of at least one NE. According to Nash's Theorem in [14]:

Theorem 1 *Every game that has a finite strategic form, with finite numbers of players and finite number of pure strategies for each player, has at least one NE involving pure or mixed strategies.*

We call a strategy *pure* when a player chooses to take one action with probability 1. *Mixed strategy* is a strategy which chooses randomly between possible moves. In other words this strategy is a probability distribution over all the possible pure strategy profiles. Since $\mathcal{G}_{\mathcal{SG}}$ (i) has a finite strategic form highlighted in Table 1, (ii) has finite number of players (MANET, malicious coalition) and (iii) has a finite number of pure strategies for each player: two for the MANET[3], two for any malicious coalition[4] satisfies the requirements of Theorem 1. Thus, $\mathcal{G}_{\mathcal{SG}}$ has at least one NE.

4. NE Derivation

In the following we have derived the NE point of $\mathcal{G}_{\mathcal{SG}}$. In other words, we have derived the strategies of both MANET and malicious coalition at NE which is the solution $(\mathbf{P_d^*}, \mathbf{P_a^*})$ of the $\mathcal{G}_{\mathcal{SG}}$.

[3] *defending*, *non-defending*
[4] *attacking*, *non attacking*

Lemma 2 *At NE, the probability of the malicious coalition to attack any node equals to p_a^* for all the different MANET nodes. Thus,*

$$p_{a,n_i}^* = p_{a,n_j}^* = p_a^* \ \forall \ i,j \in N \ s.t. \ p_{d,n_i}^*, \ p_{d,n_j}^* > 0 \tag{4}$$

and at the NE point, the MANET defends with the same likelihood p_d^* any legitimate node. In maths terms,

$$p_{d,n_i}^* = p_{d,n_j}^* = p_d^* \ \forall \ i,j \in N \ s.t. \ p_{a,n_i}^*, p_{a,n_j}^* > 0 \tag{5}$$

Consequently, we claim that the NE point of the security game is $(\mathbf{P_d^*}, \mathbf{P_a^*})$ where $\mathbf{P_d^*} = \{\underbrace{p_d^*, ..., p_d^*}_{n}\}$ and $\mathbf{P_a^*} = \{\underbrace{p_a^*, ..., p_a^*}_{n}\}$ or else Eq. (4) and Eq. (5), of Lemma 2, hold at NE. In the following we prove why the above statement is true based on the fact that at NE none of the players wants to unilaterally deviates in its strategy, as stated in Lemma 1.

Proof: First we have proven that Eq. (4) holds at NE. From Eq. (2), (4) and (5) we have that:

$$0 \leq r_d p_{a,n_i}^* - r_f cost_f - cost_d = r_d p_{a,n_j}^* - r_f cost_f - cost_d \tag{6}$$

and for any $n_k \in \mathcal{N} \ s.t. \ p_{d,n_k}^* = 0$ holds:

$$r_d p_{a,n_i}^* - r_f cost_f - cost_d \geq r_d p_{a,n_k}^* - r_f cost_f - cost_d \tag{7}$$

If the above point $(\mathbf{P_d^*}, \mathbf{P_a^*})$ is not a NE then at NE one of the following must hold; (i) $r_d p_{a,n_i}^* - r_f cost_f - cost_d < 0$. In this case the MANET has incentive to change its strategy by setting its defending probability p_{d,n_i}^* to 0 to avoid gaining negative utility. This contradicts Lemma 1; (ii) $0 \leq r_d p_{a,n_i}^* - r_f cost_f - cost_d < r_d p_{a,n_j}^* - r_f cost_f - cost_d$. In this case the MANET has incentive to change its strategy by decreasing its defending probability p_{d,n_i}^* and increase p_{d,n_j}^* as it gains higher utility when it defends the node $n_j \in \mathcal{N}$ which contradicts Lemma 1; (iii) $0 \leq r_d p_{a,n_i}^* - r_f cost_f - cost_d < r_d p_{a,n_k}^* - r_f cost_f - cost_d$. However, in this case the MANET has incentive to change its strategy by adding the defending probability p_{d,n_i}^* to p_{d,n_k}^* and set $p_{d,n}^* = 0$. This happens due to gaining higher utility when it defends the node $n_k \in \mathcal{N}$ which contradicts Lemma 1.

Thus at NE from Eq. (6) and (7) we have that Eq. (4) is true. Likewise we have proven that (5) is true at NE although we have omitted this proof here due to page limitations. Thus, at NE the utility functions of the MANET (Eq. (2)) and the malicious coalition (Eq. (3)) assuming that $V_{n_i} = V_{n_j} = V, \ \forall \ i,j \in \mathcal{N}$, become:

$$U_{manet}(\mathbf{P_d^*}, \mathbf{P_a^*}) = NV[p_d^*(r_d p_a^* - r_f cost_f - cost_d) - p_a^*]$$

$$U_{mc}(\mathbf{P_d^*}, \mathbf{P_a^*}) = Vp_a^*(-p_d^* r_d + 1 - cost_a)$$

To find the stationary point which maximises the utility functions of the MANET and the malicious coalition at NE we have the following[5]:

$$\frac{dU_{manet}(\mathbf{P_d^*}, \mathbf{P_a^*})}{d\mathbf{P_d^*}} = 0 \Leftrightarrow r_d p_a^* - r_f cost_f - cost_d = 0 \Leftrightarrow$$

[5]we use the Leibniz's notation

$$p_a^* = \begin{cases} \dfrac{r_f cost_f + cost_d}{r_d}, & r_d \geq r_f cost_f + cost_d \quad (8) \\ 1, & \text{otherwise} \quad (9) \end{cases}$$

$$\frac{dU_{mc}(\mathbf{P_d^*}, \mathbf{P_a^*})}{d\mathbf{P_a^*}} = 0 \Leftrightarrow -p_d^* r_d + 1 - cost_a = 0 \Leftrightarrow$$

$$p_d^* = \begin{cases} \dfrac{1 - cost_a}{r_d}, & r_d \geq 1 - cost_a \quad (10) \\ 1, & \text{otherwise} \quad (11) \end{cases}$$

5. Numerical Results

In this section we discuss the numerical results. At the NE point, both players (MANET and malicious coalition) reach a unique point $(\mathbf{P_d^*}, \mathbf{P_a^*}) = (\{\underbrace{p_d^*, ..., p_d^*}_{n}\}, \{\underbrace{p_a^*, ..., p_a^*}_{n}\})$ and they do not consume all of their available energy. We notice that the malicious coalition does not have any profit at NE even if it decreases its attack cost. This happens because in this case the MANET will increase its monitoring probability reducing the utility of the malicious coalition to zero. Although, the profit of the malicious coalition can be measured as the degree of damage caused to the MANET when an attack is successfully launched. This can occur due to IDS malfunction or IDS limited capabilities.

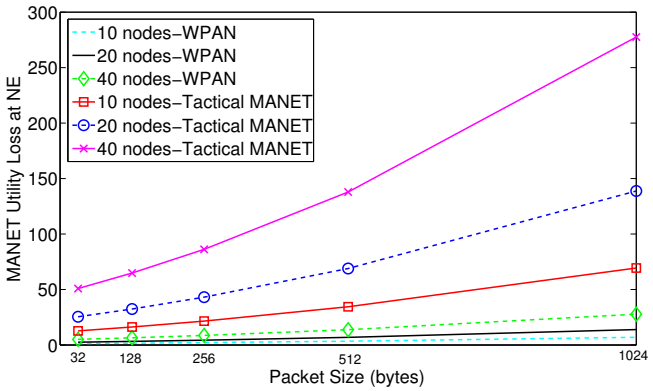

Figure 1: The MANET utility loss at NE against the packet size for different network types and sizes.

In Fig. 1 we illustrate the MANET utility loss at the NE point in terms of mJoules as a function of the packet size. We have considered two different types of MANETs; a Wireless Personal Area Network (WPAN) and a tactical MANET (i.e. emergency, military). Both network types use the same air interface. The difference between these two types is that in the case of tactical MANETs we are interested to apply high level of security even if the energy consumption is high due to the "critical" nature of these networks. On the other hand, for WPANs we are more interested in saving energy rather than applying the same level of security with the tactical networks. The MANET utility loss depends on the energy spent for intrusion detection. In other words, the MANET has to spend some energy resources to monitor the traffic within the network and recognize malicious activities. We notice from Fig. 1 that the higher the network size is the higher, the MANET utility loss is, for a specific type of network. This was expected since

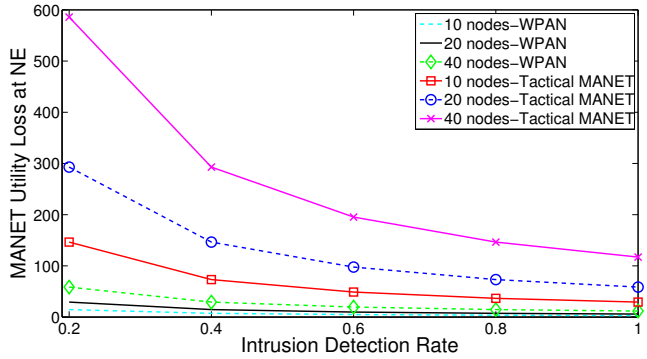

Figure 2: The MANET utility loss at NE against the intrusion detection rate for different network types and sizes.

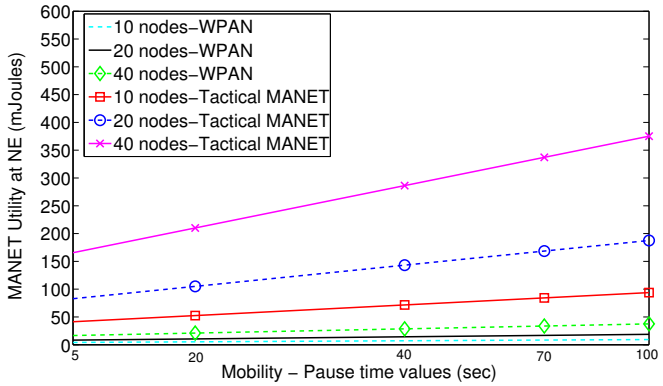

Figure 3: The MANET utility loss at NE in terms of mJoules as a function of the nodes' mobility level for different network types and sizes.

the MANET utility is the cumulative utility of all the MANET nodes meaning that higher number nodes implies higher MANET utility loss for certain packet sizes. We also see in the same figure that for a tactical MANET the utility loss is higher than for a WPAN due to the higher required security level. Eventually larger packet size introduce higher MANET utility loss due to higher energy consumption to monitor the packet and compare it with an attacking pattern.

In Fig. 2 we have depicted the MANET utility loss against the IDS rate which is an indicator of the MANET's intrusion detection capability. We observe that for increasing IDS rate the MANET utility is decreasing because more attacks are prevented thus more nodes are not damaged. We additionally see that the same trend is followed with the case of Fig. 1 regarding different types of networks and different network sizes. The MANET utility loss in the case of WPANs is less than in tactical MANETs whilst the higher network size introduces higher MANET utility loss due to the participation of more devices in the intrusion detection. It is also worth noting, from Fig. 2 that in the case where the intrusion detection rate has very small value (i.e. 0.2) the MANET utility loss is significantly high (i.e. 600 mJoules for 40 nodes tactical MANET) showing that the intrusion detection rate strongly indicates the level of the MANET utility.

Furthermore, Fig. 3 shows the MANET utility at NE for different node mobility levels or else different pause times. We notice that when mobility increases the MANET

utility loss increases. This happens due to higher number of link breakages caused by nodes movement outside the transmission range of each other. These packet errors might appear as a malicious activity (dropping packets) by the IDS. Thus, energy is spent to defend MANET against a non-existing attack. On the other hand, low mobility makes easier the detection of an attack since the IDS can collect and analyse more information regarding a certain node which actually stays within the range of its neighbours for longer period due to the low mobility.

We have also compared the average changes of a tactical MANET utility as a function of the network size. We have omitted to illustrate these results due to page limitations. The results show that for all the different network sizes the average change in the MANET utility is the same for each of the examined parameters. This can be explained since intrusion detection takes place locally or else within the same neighbourhood. This implies that even for higher network size the improvement or detriment of the MANET utility function due to varying parameters such as packet size, mobility and IDS rate is almost the same. For incremental detection rate (i.e. 20, 40, 60, 80, 100%) the MANET utility's improvement percent is almost 30%. This implies that when the quality of the IDS (in terms of hardware or software) is improved (detecting more malicious activities), the increment in the MANET utility is significant. For incremental mobility the detriment of the utility is approximately 4% whilst for incremental packet size the corresponding detriment is 30%. This signifies that the changes in mobility and packet size during the network's lifetime do not equally affect the MANET utility. The high impact of the packet size indicates that applications must be carefully chosen to support nodes' communication in a tactical MANET. On the other hand, the small value of utility's detriment in the case of changing mobility shows that the intrusion detection will afford any gradual changes in the pause time of the MANET nodes.

It is worth mentioning that, we were anticipating the negative $U_{manet}(\mathbf{P_d^*}, \mathbf{P_a^*})$'s value at the NE point due to the energy spent by the IDS. In addition, we see that spending more energy resources (case of incremental $cost_d$) causes degradation of MANET's utility function. Also, to reduce the damage caused by attacks, MANET has to improve its IDS performance or else to increase its intrusion detection rate. To summarise, the $U_{manet}(\mathbf{P_d^*}, \mathbf{P_a^*})$ increases in the following cases; (i) the detection rate increases; (ii) the false alarm detection decreases, (iii) the intrusion detection cost decreases, (iv) the false alarm cost decreases.

6. Conclusion

In this paper we use game theory to model non-cooperative security games between a MANET, which is defended by IDS operating at each node as well as a group of collaborative malicious nodes called *malicious coalition*. Our work innovates by finding the defending and attacking probability distributions, of any MANET and malicious coalition, that maximise the utility of the players at the Nash Equilibrium (NE) of a non-cooperative security game between the aforementioned entities.

To this end, one of the main objectives of this paper was to design the utility functions of both players. We have designed the utility of the MANET as a function of: (i) the attack detection rate, (ii) the security loss due to a successful attack, (iii) the cost for a false alarm, (iv) the rate of a false alarm and (v) the cost of defending a MANET node. On the other hand, we have designed the utility of the malicious coalition as a

function of: (i) the attack detection rate, (ii) the security loss for a legitimate MANET node when the attacker succeeds to harm this node and (iii) the cost of attacking a MANET node.

Based on this design we have derived the NE of the non-cooperative security game and we have proven its validity. In fact, we have shown that at the NE point, the MANET and the malicious coalition have to equally distribute their defending and attacking probabilities correspondingly. To this end, we have used the *Nash theorem* as well as the contradiction method to prove that in any case that the attacking and defending probabilities are not equally distributed, the MANET and the attacker have motivation to change their behaviours in order to increase their utility functions. According to the definition of the NE, any player of the game does not deviate from its behaviour at NE which in our security game means that in a non-NE point the MANET will prefer to increase the defending probability of a node j and decreasing the defending probability of a node i. In addition, in some cases where the defending probabilities are not equal the MANET prefers not to defend some nodes in order to avoid gaining negative utility. We have observed the same trend regarding the attacking probabilities, as discussed in this paper. The results about the aforementioned probability distributions align with the fact that the legitimate MANET nodes are considered equally important for the network's operation and the attacker realises that each MANET node which might be successfully attacked will harm the network as much as any other node. By maximising the utility function at the NE we have derived the optimised defending and attacking probability distributions as functions of the false alarm rate and cost, the detection cost, the detection rate and finally the attacking cost. The different parameters critically affect the final defending and attacking distribution probabilities as we have shown in this paper.

To go a step further, this paper proposes a way to derive the intrusion detection or the attack effort respecting the corresponding energy costs of the MANET and the malicious coalition. It is worth stressing here that at the NE we have noticed that the MANET and the malicious do not spend all of the available energy. In addition the malicious coalition does not have any definite security benefit when it somehow reduces its attacking cost at the NE if the MANET increases its defending probability. The only gain for the attacker in that case is the fact that the MANET nodes might drain their batteries faster since more energy is spend when the defending probability is higher. In other words, an attacker expects to gain some security benefits only if the intrusion detection systems within the MANET area do not detect any malicious activity.

Numerical results have been illustrated showing the changes at MANET's utility, at NE, as a function of the packet size, the intrusion detection rate and the mobility of the MANET nodes. We have considered two MANET types, namely WPAN in which energy consumption is the main concern and tactical MANETs which require high level of security. From these results, we have noticed that larger packet size introduces higher MANET utility loss. In addition, for increasing detection rate the MANET utility decreases and in the case of a WPAN the MANET utility loss is less than in tactical MANETs. Regarding the mobility level, we have concluded that for higher MANET node mobility the MANET utility loss is higher due to the higher number of packet errors (e.g. due to breakage links) which might be treated as a denial of service attack by the IDS enabling a false alarm. On the other hand, low mobility levels allow the IDS to collect more data towards the correct recognition of an attack.

Our plans for future work include but are not limited to simulate a scenario where malicious nodes launch attacks against the MANET nodes whilst the latter are using intrusion detection techniques to recognise such attacks spending faster their residual energy. In such a work we will focus on maximising the intrusion detection sampling rate using the results of this paper to achieve an efficient balance between the intrusion detection as well as the implied energy consumption.

References

[1] E. Panaousis, A. Ramrekha, K. Birkos, C. Papageorgiou, V. Talooki, G. Matthew, C. Nguyen, C. Sieux, C. Politis, T. Dagiuklas, *et al.*, "A framework supporting extreme emergency services," in *Proc. IEEE MobileSummit*, (Sadanter, Spain), pp. 10–12, Jun. 2009.

[2] Y. Zhang and W. Lee, "Intrusion detection in wireless ad-hoc networks," in *Proc. ACM MOBIHOC*, pp. 275–283, 2000.

[3] A. Lauf, R. Peters, and W. Robinson, "A distributed intrusion detection system for resource-constrained devices in ad-hoc networks," *Ad Hoc Netw.*, vol. 8, no. 3, pp. 253–266, 2010.

[4] A. Patcha and J. Park, "A game theoretic formulation for intrusion detection in mobile ad hoc networks," *Int. Journ. of Netw. Sec.*, vol. 2, no. 2, pp. 131–137, 2006.

[5] H. Otrok, N. Mohammed, L. Wang, M. Debbabi, and P. Bhattacharya, "A game-theoretic intrusion detection model for mobile ad hoc networks," *Comp. Comm.*, vol. 31, no. 4, pp. 708 – 721, 2008. Algorithmic and Theoretical Aspects of Wireless ad hoc and Sensor Networks.

[6] E. Panaousis and C. Politis, "A game theoretic approach for securing aodv in emergency mobile ad hoc networks," in *Proc. 34th IEEE Conference on Local Computer Networks (LCN)*, (Zurich, Switzerland), pp. 985–992, Oct. 2009.

[7] Z. Ji, W. Yu, and K. Liu, "A belief evaluation framework in autonomous manets under noisy and imperfect observation: Vulnerability analysis and cooperation enforcement," *IEEE Trans. Mobile Comput.*, vol. 9, pp. 1242 –1254, Sep. 2010.

[8] Y. Liu, C. Comaniciu, and H. Man, "A bayesian game approach for intrusion detection in wireless ad hoc networks," in *Proc. GAMENETS*, (NY, USA), p. 4, 2006.

[9] F. Li, Y. Yang, and J. Wu, "Attack and flee: Game-theory-based analysis on interactions among nodes in manets," *IEEE Trans. Syst., Man, Cybern. (B)*, vol. 40, pp. 612 –622, Jun. 2010.

[10] W. Yu and K. Liu, "Game theoretic analysis of cooperation stimulation and security in autonomous mobile ad hoc networks," *IEEE Trans. Mobile Comput.*, vol. 6, pp. 507 –521, May 2007.

[11] W. Yu, Z. Ji, and K. Liu, "Securing cooperative ad-hoc networks under noise and imperfect monitoring: Strategies and game theoretic analysis," *IEEE Trans. Inf. Forensics Security*, vol. 2, pp. 240 –253, Jun. 2007.

[12] M. Osborne and A. Rubinstein, *A course in game theory*. The MIT press, 1994.

[13] N. Nisan, T. Roughgarden, E. Tardos, and V. V. Vazirani, *Algorithmic Game Theory*. New York, NY, USA: Cambridge University Press, 2007.

[14] J. Nash, "Non-cooperative games," *Annals of mathematics*, vol. 54, no. 2, pp. 286–295, 1951.