A Game Theoretic Approach for Securing AODV in Emergency Mobile Ad Hoc Networks

Emmanouil A. Panaousis and Christos Politis
Wireless Multimedia & Networking (WMN) Research Group
Kingston University London
KT1 2EE London, United Kingdom
{e.panaousis, c.politis}@kingston.ac.uk

***Abstract*—In many extreme emergency cases such as forest fires or tube terrorist attacks, the rescuers have difficulty using traditional legacy networks due to destruction or collapse of the infrastructure in such events. We use the term emergency Mobile Ad hoc NETworks (eMANETs) in order to describe Next Generation Networks (NGNs) which are deployed in emergency cases. The security of these networks is critical. Especially secure routing is important given the fact that potential attackers aim to disrupt the appropriate operation of the routing protocol within an eMANET.ŁIn this paper we propose a game theoretic approach called AODV-GT (AODV-Game Theoretic) and we integrate this into the reactive Ad hoc On-demand Distance Vector (AODV) routing protocol to provide defense against blackhole attacks. AODV-GT is based on the concept of non-cooperative game theory. AODV-GT outperforms AODV in terms of malicious dropped packets when blackhole nodes exist within the eMANET. Our simulations were implemented using the network simulator ns-2.**

I. Introduction

Wireless networking technologies are an appropriate foundation to support different rescuers in an emergency situation such as a forest fire or a tube terrorist attack. In a disaster case, each rescue team (police team, fire working team, ambulance team, etc.) has to be aware about the situation and all the teams have to collaborate and communicate.

The EU-FP7 PEACE project[1] investigates the provisioning of day-to-day emergency communications in next generation all-IP networks. One scenario examined by PEACE is how to supply the policemen and firemen with an enhanced PDA or personal digital assistant. Therefore the idea is to use an "intelligent" device to achieve secure and reliable communications when traditional networks have failed. One of the major technological challenges PEACE will be addressing is the implementation of a general solution for secure multimedia communication in extreme emergency situations. Our proposed methodology is part of the PEACE Security Platform (PSP) proposed in [1] and [2]. PSP will be a platform of secure protocols of network, transport and application layers, developed for the purposes of PEACE.

The nature of MANETs[2] makes them suitable to be utilized in the context of an emergency case for various rescue teams as we depict in figure 1[3]. Due to their flexibility and self-organization capabilities, MANETs are well suited for scenarios where certain network services such as message routing and event notification have to be provided quickly and dynamically without any centralized infrastructure. For instance we can have situations where potentially large numbers of recovery workers from multiple organizations must cooperate and coordinate in areas where natural or man-made disasters have damaged much of the infrastructure including the telecommunications services.

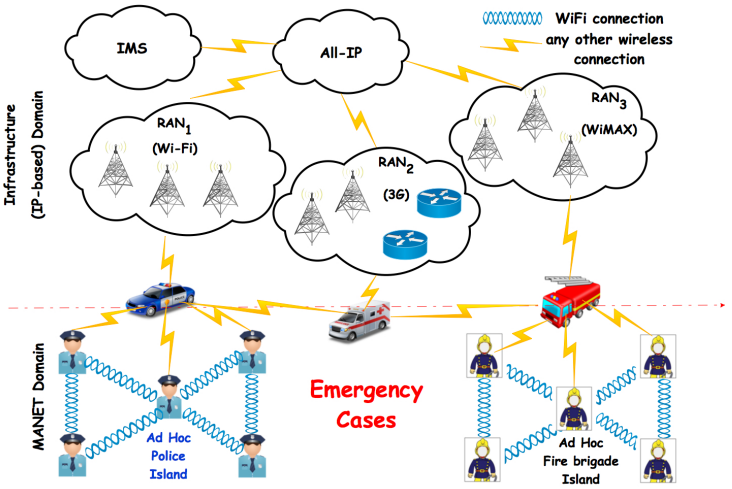

Fig. 1. An example when MANETs are deployed to support the various working teams in emergency cases such as forest fires or terrorist attacks.

The inherently vulnerable characteristics of MANETs make them susceptible to attacks and counter attacks might end up being too little too late. Traditional security measures are not applicable in MANETs due to the following reasons: (i) MANETs do not have infrastructure nature due to the absence of centralized authority, (ii) MANETs do not have grounds for an "a priori" classification due to the fact that all nodes are required to cooperate in supporting the network operation, (iii) wireless attacks may come from all directions within a

[1]PEACE is a partly funded EU project. For more info visit: http://www.ict-peace.eu/.

[2]from now on we use both terms MANETs and eMANETs for the same scope.

[3]when is needed connection could be established between the infrastructure domain and the MANET domain.

MANET, (iv) wireless data transmission does not provide clear line of defense, gateways and firewalls and (v) MANETs have constantly changing topology owing to the movement of nodes in and out of the network.

Especially, the MANET security is one critical part of PEACE project because aim of the legitimate nodes is to adapt high level defending mechanisms in order to protect sensitive information and to maintain the appropriate operation of the MANET communications in emergency cases.

In this work we propose a methodology, for securing the reactive Ad hoc On-demand Distance Vector (AODV) routing protocol, called AODV-GT (AODV- Game Theoretic). The latter is an effective in terms of Intrusion Detection Systems' (IDS) [3] computational cost routing protocol. Additionally, AODV-GT decreases the probabilities the potential malicious node have to damage a high number of communication links. The methodology is effective due to the fact that implements routing in a way that the utility function of the MANET is maximized. In addition, we prove that the emerging two-player game between the eMANET and each of the blackhole nodes converges to a Nash Equilibrium (NE) point when AODV-GT is applied.

It is worth mentioning here the concept of IDS. This is important for the security of a MANET due to the fact that it could be a second wall of defense when prevention mechanisms have failed. If there are attacks on a system, one would like to detect them as soon as possible and take an appropriate action. According to [4] there are two main types of intrusion detection systems:

- host-based IDS (HIDS) which run on a host and they focus on collecting data on each host in most cases through operating system audit logs
- network-based IDS (NIDS) which do not run on each host but on some areas within the MANET.

In our work, we consider the HIDS approach. Once the data are collected by the HIDS sensors, they have to be analyzed in order to detect malicious activities. Thereafter, actions will be taken automatically in order to stop the attack.

This paper is organized as follows. In section II we introduce the concept of secure routing in MANETs and we discuss fundamental concepts related with our work. In Section III we describe the AODV-GT. Section IV includes the simulation results. We conclude this paper in section V and we discuss our plans for future work.

II. Background

A. Routing

Routing is an important function of any MANET given the fact that the nodes play the role of routers[4]. Therefore, the implementation of routing protocols is essential requirement whilst we need to guarantee that these protocols are secure. For the purposes of PEACE project we use either the proactive Optimized Link State Routing (OLSR) protocol or the reactive AODV routing protocol. The choice of these two protocols is based on the research published in [5] which shows that OLSR and AODV are the most attractive for an adaptive solution for multimedia transmission. In addition, we have developed and published in [6] a new hybrid routing protocol for eMANETs called ChaMeLeon (CML). The protocol is designed to adapt its routing behavior according to the size of an eMANET. The reactive AODV and the proactive OLSR are deemed appropriate for CML through their performance evaluation in terms of delay and jitter for different MANET sizes and different kind of node mobility models.

The disadvantage of the most ratified routing protocols for MANETs is the fact that they have been developed without considering security mechanisms in advance. The case becomes more critical when extreme emergency communications must be deployed at the ground of a rescue. In these cases adversaries could launch different kind of attacks damaging the quality of the communications. However several secure routing protocols have been proposed in bibliography in accordance with our knowledge a significant small number of them is based on game theory. For instance, authors in [7] propose an original security mechanism called CORE which is based on reputation that is used to enforce cooperation among the nodes of a MANET. Authors use game theory to model the interactions between the nodes of the ad hoc network. In [8] authors present a joint analysis of cooperative stimulation and security in autonomous MANETs under a game theoretic framework.

B. Blackhole Attack

A blackhole attack is a kind of Denial-of-Service (DoS) attack accomplished by dropping packets. In figure 2, we show a case where two malicious nodes launch blackhole attacks succeeding to drop packets within the MANET. The blackhole problem in MANETs is a critical security problem given the fact that one or more malicious nodes use the routing protocol to advertise themselves as having the shortest path to the node whose packets they want to intercept. An attacker launches a blackhole attack by replying to every routing request very fast, pretending that it has a route to the destination node. After the launching of a blackhole attack, the malicious node has the potential to drop the packets or to use its place on the route in order to launch a man-in-the-middle attack. The packet dropping may be selective affecting only a particular type of packets or not. The effectiveness of a blackhole attack is based on the fact that in AODV, the source node uses the first route which it receives in order to transmit its packets to the destination node. Due to the fact that a malicious node does not have to check its routing table[5], it is the first node that responds to the Route REQuest (RREQ) by sending a Route REPly (RREP) to the source node.

C. Game Theoretic Aspects

Game theory [9] is a scientific area that aims to model situations in which decision makers have to make specific

[4]as we have mentioned this occurs due to the absence of centralized infrastructure.

[5]as legitimate nodes do.

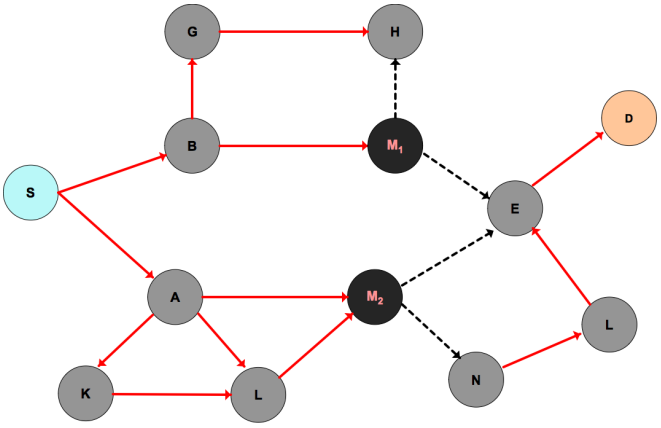

Fig. 2. An example of a MANET where blackhole nodes damage the routing function by dropping packets.

actions with mutual and possibly conflicting consequences. Game theory is also a branch of mathematics which has been explored fairly recently within the last century. The ideas presented in game theory are useful in outlining what the best decision making techniques are in certain situations. The basic assumptions that underlie the theory: (i) the decision makers are rational and (ii) they reason strategically which means they take into account their knowledge or expectations of other decision makers. The essential elements of a game are the players, the actions, the payoffs and the information, known collectively as the *rules* of the game. A solution of a two-player game[6] 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) [9]. At a NE, given the strategies of other players, no user can improve its utility level by making individual changes in its strategy.

In terms of mathematics, let (S, U) be a game, where S is the set of *strategy profiles* and 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, a strategy profile $s^* \in S^*$ is a NE if no unilateral deviation in strategy by any single player is profitable or:

$$\forall \ i, \ u_i(s_i^*, s_{-i}^*) \geq u_i(s_i, s_{-i}^*) \tag{2}$$

In our work, we propose a non-cooperative *non-zero sum game* theoretic approach. In game theory a zero-sum game highlights a situation in which a player's gain or loss is exactly balanced by the losses or gains of the other players. In order to find the NE in a non-zero sum game we have to consider the concept of the *dominant strategy*. A strategy is called dominant when it is better than any other strategy for one player, no matter how that player's opponents could play.

In terms of mathematics, for any player i, a strategy $s^* \in S_i$ dominates another strategy $s^{'} \in S_i$ if $\forall \ s_{-i} \in S_i$:

$$u_i(s^*, s_{-i}) \geq u_i(s^{'}, s_{-i}) \tag{3}$$

Theorem 1 (Nash-Theorem): 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 strategy* 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. The game we examine satisfies the assumptions of the Nash theorem which means that a NE exists in that game.

III. Proposed Methodology

In this section, we define the emerging non-cooperative game between the MANET and potential blackhole nodes and we describe our proposed methodology called AODV-GT[7]. About the former, we study a two-player non-cooperative non-zero sum route selection game in order to forward the packets of the legitimate nodes across the MANET. Furthermore, we describe the potential non-cooperative strategies of each player.

In figure 2 we show a MANET scenario where two malicious nodes M_1, M_2 are trying to launch blackhole attacks. Specifically, the adversaries have the potential to advertise shorter routes to a destination node. As a result the source nodes believe that their packets should be passed through the nodes M_1, M_2. In this case, the function of the routing protocol has been disrupted. Later on, the malicious nodes succeed in dropping a significant number of packets.

In accordance with our methodology, we will formulate the described situation using a game theoretic framework. The players of the game are (i) the MANET and (ii) a blackhole node. Thus, a two-player game is emerging. The game reaches a NE as we will show later on. The concept could be generalized for n blackhole nodes assuming all the two-player games between the MANET and each malicious node.

Our methodology has been inspired by the work done in [10]. The authors examine security issues in wireless sensor networks which are divided in a number of clusters. Each cluster head-node of a cluster finds a route to another cluster using the Dynamic Source Routing protocol (DSR) [11]. In this work the MANET is responsible for defending the cluster

[6]we mention the two-player game because later on we will formulate a two-player game with players the MANET a blackhole node.

[7]and how this is applied within AODV.

head-nodes against malicious nodes which launch DoS or spoofing attacks.

In our work we examine especially the case of a non-cooperative game where the MANET tries to defend the most critical[8] route among all the routes that are delivered to the source node by the AODV protocol [12]. On the other hand, malicious nodes try to launch blackhole attacks on these routes. Towards the formulation of our game we define the strategy space for each player.

- strategy space of the MANET:
  - d_i: the MANET defends a route i
  - d_{-i}: the MANET defends any other route $-i$.
- strategy space of a blackhole node:
  - m_i: the blackhole node attacks a route i
  - m_0: the blackhole node does not attack MANET
  - m_h: the blackhole node attacks a route h.

Therefore, the MANET has the potential to play:

$$D = \begin{pmatrix} d_i & d_i & d_{-i} \end{pmatrix}$$

and each malicious node:

$$M = \begin{pmatrix} m_i \\ m_0 \\ m_h \end{pmatrix}$$

In table I we show the payoff matrix of the MANET. In the table we use the abbreviation s.t. which stands for *strategy tuples*.

TABLE I
PAYOFF MATRIX OF MANET

s.t.	m_i	m_0	m_h
d_i	$PD(t) - DC_i$	$PD(t) - DC_i$	$PD(t) - DC_i - -FC_h$, for $h \neq i$
d_{-i}	$PD(t) - DC_{-i} - -FC_i$	$PD(t) - DC_{-i}$	$PD(t) - DC_{-i} - -FC_h$ for $h \neq i, -i$

$PD(t)$ is the utility of the MANET at time t, DC_i is the cost for defending a route i and FC_i is the cost of failing to protect the route i. In addition, we define the number of one-hop neighbors of a node j as nn_j. Especially, DC_i depends on the values of $nn_j \ \forall \ j \in i$ and it is equal to:

$$DC_i = \frac{\sum_{j \in i} nn_j}{n_i} \tag{4}$$

where n_i is the number of nodes which constitute the route i. More precisely, the cost of defending a route against a malicious node is actually the cost of operating the HIDS sensors in the nodes which constitute this route as well as in the one-hop neighbors of these nodes. The latter could hear the transmissions and they could participate in the intrusion detection. Obviously, when a packet is forwarded through a route which has higher DC_i value than another route, the cost for defending the former route is higher due to the participation of more HIDS sensors.[9] At the same time, according to equation (4) when DC_i is minimized the number of nodes that a blackhole node has the potential to damage is minimized too.

The value of FC_i changes as a function of the density of the mobile nodes that constitute a route. The cost of failing to protect a route i is equal to the utility value that the attacker gains by dropping packets on this route. A malicious node which communicates in a small region with a high number of legitimate nodes[10] has higher possibility to gain better utility value by launching a blackhole attack. In other words, when a route is comprised of nodes with low density, the blackhole node is less interested to place itself on this route due to the fact that it cannot damage so many nodes as it would have done if it was on a route of higher density. We define the metric of density for each node j, according to [13], as follows:

$$dens_j(R) = \frac{NR_j^2\pi}{A} \tag{5}$$

where R_j is the radio transmission range of the node j, N is the number of nodes within the transmission range of node j at time t and A is the size of the region of the MANET. Therefore, we define:

$$FC_i = \frac{\sum_{j \in i} dens_j}{n_i} \tag{6}$$

In keeping with the concept of game formulation, the utility function of a malicious node is given in table II. CA_i is the cost of any attack against a route i and $PA(t)$ is the profit of each successful attack at time t.

TABLE II
PAYOFF MATRIX OF MALICIOUS NODES

s.t.	m_i	m_0	m_h
d_i	$PA(t) - CA_i$	0	$PA(t) - CA_h$, for $h \neq i$
d_{-i}	$PA(t) - CA_i$	0	$PA(t) - CA_h$, for $h \neq i$

It is worth mentioning why our game is a non-zero sum game. From the payoff matrices of the players we observe that even if the attacker does not attack the MANET is defending. The payoff of the latter therefore decreases while the payoff of the malicious node is steady. The above assumption contradicts with the zero-sum assumption which means that our game is a non-zero sum game. As we have mentioned in section II, in this kind of games the NE has to be found considering the concept of the dominant strategy.

[8]we will define later on what we mean with the expression most critical route.

[9]In addition, we could potentially suppose that DC_i depends on the degree of importance of each route too. However, for reasons of simplicity and without loss of the generality, in this work we suppose that all the routes have the same degree of importance.

[10]in this situation the value of $dens$ is high.

In order to find the NE of our game, first, we set the values d_1, d_2, d_3 in the array D for the MANET as follows:

$$D^{\star} = \begin{pmatrix} d_1 & d_2 & d_3 \end{pmatrix}$$

and we do the same in the array M:

$$M^{\star} = \begin{pmatrix} m_1 \\ m_2 \\ m_3 \end{pmatrix}$$

In our game, at the NE, the MANET chooses to defend the route with the highest value $U(t) - DC_i$. On the other hand, any blackhole node prefers to attack the MANET in order not to receive utility equal to 0.

As we have discussed, for the maximization of $U(t) - DC_i$ we need to minimize the value of DC_i. Therefore, what we need first is to find the NE of the non-cooperative non-zero sum game and then to define a utility function which will be the criterion of AODV-GT for the selection of the most secure and cost effective, in terms of IDS computational cost, route. In order to find the NE, we need to find the dominant strategy[11] of the game. The payoff matrices of the MANET and any blackhole node are $D = [d_{xy}]_{2\times 3}$ and $M = [m_{xy}]_{2\times 3}$, respectively. According to the table I we will have that:

$$d_{11}, d_{12} \geq d_{13} \tag{7}$$

Obviously, for the MANET we have that: (i) if $DC_i > DC_{-i}$ then $U(t) - DC_i < U(t) - DC_{-i} \Rightarrow d_{12} > d_{11}$ and (ii) if $DC_i < DC_{-i}$ then $U(t) - DC_i > U(t) - DC_{-i} \Rightarrow d_{11} > d_{12}$. In accordance with the table II:

$$m_{11} = m_{13} \geq m_{12} \tag{8}$$

From the above and from the definition of the dominant strategy, the strategy pair (d_1, m_1) is the NE of our game.

A. Applying AODV-GT in the AODV protocol

In this part of this paper, we describe how AODV-GT is integrate into the AODV protocol. We assume that a node S wants to find out a route to a node D. According to AODV, if S does not have a route to D, it has to send a RREQ message to its one-hop neighbors. Every node A which receives a RREQ derives the utility value $u_A = \frac{1}{nn_A}$. A has to add the value of u_A to the current utility value of the AODV packet as well as to add its IP address to the packet. If A does not have a route to D it forwards the packet according to AODV. On the other hand, if A has a route to D, first it has to add its utility value u_A to the utility value of the route $A, ..., D$ in order to derive the utility u_{AD}.

Second, A adds the value of u_{AD} to the current utility value of the AODV packet. Then, it adds its IP address to the source route and sends a RREP to S through the reverse route according to AODV. Finally, if A is the destination node D, it has only to add its utility value to the current utility value of the AODV packet and to send back to S a RREP including itself as the destination node.

[11]as we described in section II.

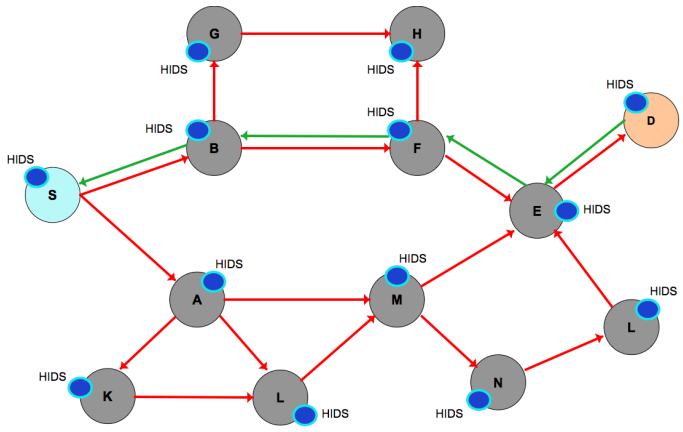

Fig. 3. The routing procedure according to AODV-GT. The source node sends its data through the route with the highest utility. The HIDS sensors monitor the route in order to collect information and detect malicious activities.

According to AODV, S sends its packets to D using the route which it receives first. In other words, S saves only one route to D. According to AODV-GT, S has to save all the routes which it receives. For this purpose, S is waiting for a *timeout* to receive all the potential routes. We set the value of *timeout* equal to Net Traversal Time (NetTT). According to [12], this is the maximum time in milliseconds waiting for the receiving of a RREP after the sending of a RREQ. In the next step, S derives the average value $\bar{u_i}$ of each route i which has cached using the following equation:

$$\bar{u_i} = \frac{nhops_i + 1}{\sum_{j \in i} nn_j} \tag{9}$$

The $nhops_i$ value indicates the number of hops which is included in the AODV packet [12]. The number of hops is the only mutable information of the packet in the AODV packet [12]. Every node which is included in the route i has to increase the hop count by 1 during the traversing of the message from D to S. Obviously, $n_i = nhops_i + 1$ where n_i is the number of nodes on a route i.

After the computation of the average utility value of each received route, S has to send its packets to D through the route which has the maximum average utility value. This route is the most secure and cost effective route in terms of HIDS sensors computational cost among all the available routes to D due to the fact that it maximizes the utility of the MANET when the game reaches the NE. In order to combat potential broken links the proposed methodology should follow the next approach. S instead of calculating only the route with the maximum average utility, it sorts in a descent manner based on the average utility all the received routes. In this way, if the route with the maximum average utility is broken, S has to select the next route from the sorted list.

A potential emerging question is how does S know about a broken link? We modify the AODV protocol appropriately in a way that each intermediate (relay) node notifies S that a link is broken. This occurs using Route ERRor (RERR) messages. The same approach is followed by the Dynamic Manet On-

demand (DYMO) routing protocol [14]. Additionally, it is worth mentioning that incase only one route is received by S, the latter sends to D using this unique route.

Specifically, the utility of the MANET at the NE is equal to:

$$U(t) - DC_i = U(t) - \frac{\sum_{j \in i} nn_j}{n_i} = U(t) - \frac{\sum_{j \in i} nn_j}{nhops_i + 1} \quad (10)$$

We integrate within the AODV protocol our proposed methodology as we show in algorithms 1 and 2.

Algorithm 1 AODV-GT (node S sends a RREQ)

if a node A receives a RREQ **then**
  if A does not have a route to the destination node D **then**
    derives u_A
    adds u_A to the current utility value in the AODV packet
    adds itself to the source route
    forwards the RREQ according to AODV
  else
    if A has a route to D **then**
      derives u_A
      adds its utility value u_A to the utility value of the route $A, .., D$ in order to compute a final utility u_{AD}
      adds u_{AD} to the current utility value in the AODV packet
      adds itself to the source route
      sends a RREP to S according to AODV
    else
      // *A is the destination node D*
      derives u_D
      adds u_D to the current utility value in the AODV packet
      adds itself as the destination node to the source route
      sends a RREP to S according to AODV
    end if
  end if
end if

Algorithm 2 AODV-GT (node S receives RREP)

S is waiting for RREP for a *timeout* NetTT
if S receives more than one RREP **then**
  S calculates the average average utility $\bar{u_i}$ of each route i
  S sorts all the received routes in a descent manner based on the average utility $\bar{u_i}$ of each route i
  S chooses the route x with the maximum average utility $\max \bar{u}_x$
  while Timeout of AODV route discovery is not expired **do**
    if the current selected route x does not include a broken link **then**
      // *this is indicated by the receiving of an RERR*
      S sends its packets to D through x
    else
      S chooses the *next route* from the sorted list to send its packets to D
      // $x :=$ *next route*
    end if
  end while
  // S receives only one RREP
  S sends its packets to D through the route which it received by the unique RREP
end if

IV. Simulation Results

In our simulations we used the network simulator ns-2. For the physical layer propagation model we used the two-way ground model with obstacles. In the MAC layer we used the IEEE 802.11b protocol.

The mobility was simulated using the Mission Critical Mobility (MCM) [15] model for ns-2. MCM implements the two-way ground propagation model and the Random Waypoint mobility model considering obstacles. MCM is a mobility model that captures the properties of the mobility of the nodes (firemen, policemen, medics, etc.) of eMANETs[12]. The MCM model is proposed in the context of PEACE and it is available in [16].

Furthermore, we used pause time equal to 20 seconds and two values of nodes' speed namely 1 and 5 meters/second. We simulated two areas which are equal to 1000 meters(m) x 1000m and 1500m x 1500m for 2000 seconds. We also generated both UDP and TCP traffic and we examined the cases of 8, 24, 32 and 44 mobile nodes. One third of each number of mobile nodes are blackhole nodes namely we simulated 2, 6, 8, and 11 malicious nodes for each of the above scenarios, correspondingly. Furhtermore, we simulated 2 application usage cases:

- each wireless node transfers data using FTP over TCP to another mobile node
- each wireless node sets up a VoIP session with another node. VoIP traffic is bidirectional and we have assumed that the G.729 voice coded is used, without silence suppression. This generates CBR traffic, carried over UDP. Every VoIP packet has 32 bytes of payload.

It is worth mentioning that even if we do not have blackhole nodes within MANET, a number of dropped packets remains due to failures of the wireless communications links. The situation becomes worst in our case due to the fact that we assumed the existence of obstacles. The latter introduce higher difficulty in the delivery of the packets compared to the pure two-way ground model. Obviously, when malicious nodes exist, the number of dropped packets is higher. After the application of our mechanism the number of dropped packets is decreased though it can not reach the case without malicious nodes. This occurs due to the fact that an HIDS need some time before reacting to an attack. Obviously, this is the time to detect this attack. In addition, depending on the thresholds (see [4]) which have been set at the HIDS sensors for the detection of the attacks, there is different degree of accuracy in recognizing the malicious activities.

In figures 4, 6, 8 and 10 we show the ratio of dropped packets per received packets as a function of the total number of nodes for FTP over TCP traffic for the different simulation parameters. In figures 5, 7, 9 and 11 we highlight the corresponding results for VoIP traffic. Due to the fact that TCP is a connection-oriented protocol the number of dropped packet due to link failures is less than in UDP which is a connectionless protocol. In both cases AODV-GT improves the ratio of dropped per received packets optimizing the computational cost of IDSs[13]. We notice that the results are better in the area of 1500m x 1500m than in the 1000m x 1000m area due to the fact that blackhole nodes achieve to drop less packets when the density of the MANET is lower.

[12] deployed in mission critical situations like earthquakes, forest fires, floods, miltary operations, etc.

[13] at NE.

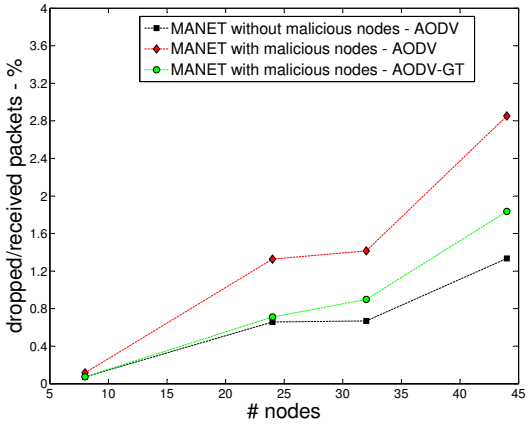

Fig. 4. Percentage of dropped packets for FTP traffic in a 1000m x 1000m area for 1m/s speed of nodes.

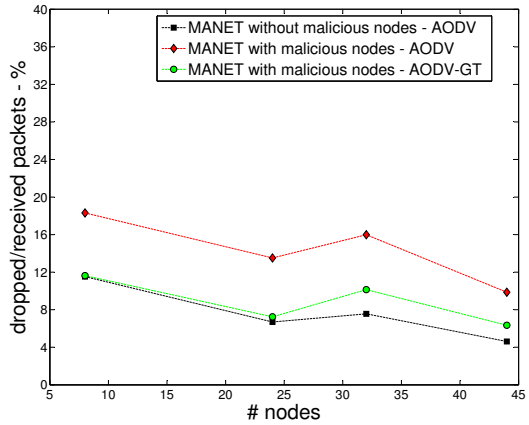

Fig. 5. Percentage of dropped packets for VoIP traffic in a 1000m x 1000m area for 1m/s speed of nodes.

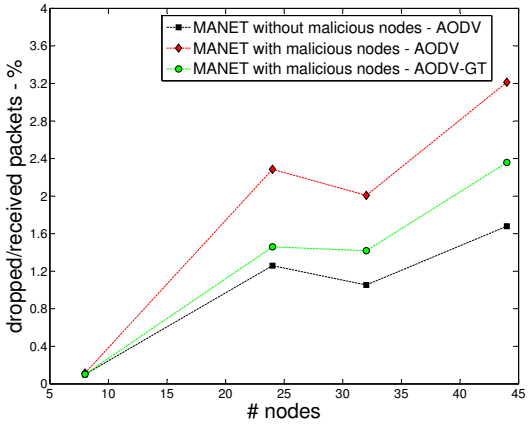

Fig. 6. Percentage of dropped packets for FTP traffic in a 1000m x 1000m area for 5m/s speed of nodes.

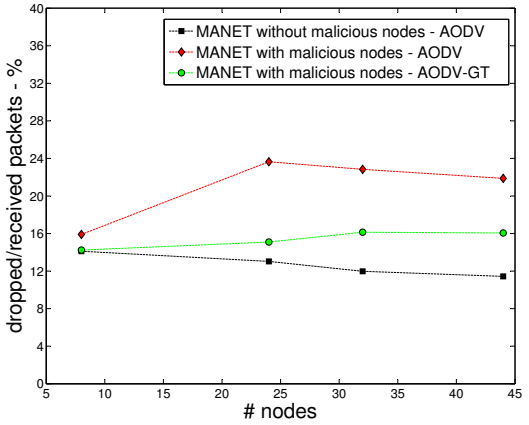

Fig. 7. Percentage of dropped packets for VoIP traffic in a 1000m x 1000m area for 5m/s speed of nodes.

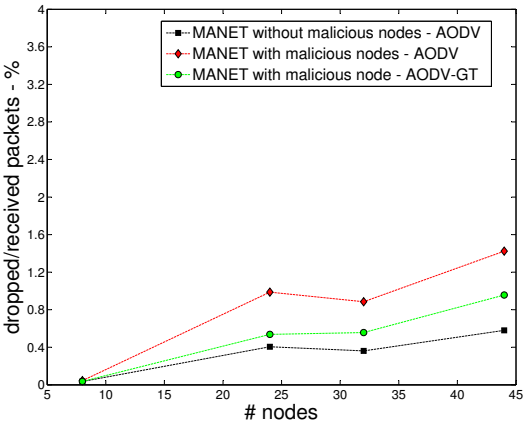

Fig. 8. Percentage of dropped packets for FTP traffic in a 1500m x 1500m area for 1m/s speed of nodes.

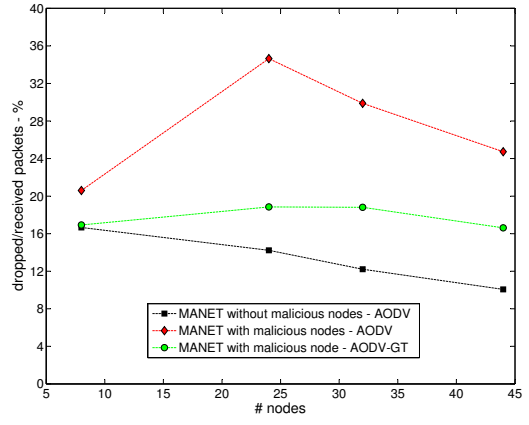

Fig. 9. Percentage of dropped packets for VoIP traffic in a 1500m x 1500m area for 1m/s speed of nodes.

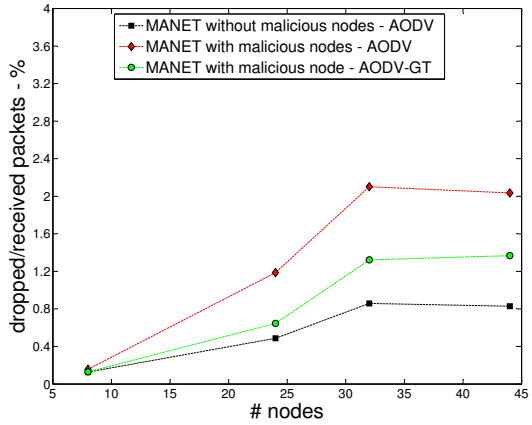

Fig. 10. Percentage of dropped packets for FTP traffic in a 1500m x 1500m area for 5m/s speed of nodes.

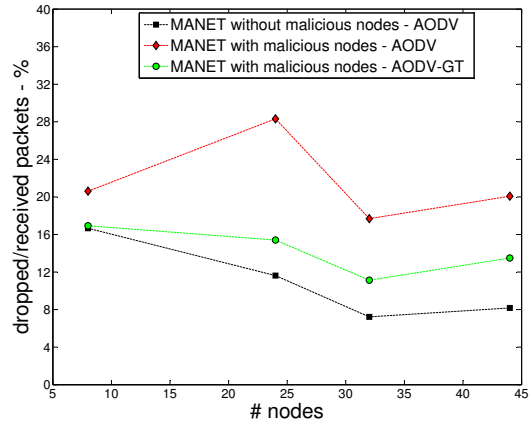

Fig. 11. Percentage of dropped packets for VoIP traffic in a 1500m x 1500m area for 5m/s speed of nodes.

V. Conclusions and Future Work

In this paper we proposed a game theoretic approach called AODV-GT and we integrated it into the AODV protocol for securing AODV in emergency Mobile Ad hoc NETworks (eMANETs) against blackhole attacks. The simulation results show that AODV-GT outperforms AODV in terms of dropped per received packets for different number of blackhole nodes within our eMANET.

We additionally supposed HIDS sensors which are able to detect the malicious nodes and excluding them from the eMANET. The scope is of this work however is not to explain the function of HIDS but to propose the AODV-GT approach as it was described extensively in this paper.

To this end, we formulated a game between the eMANET and each potential blackhole node. We found the NE and we showed that the most effective route to forward the packets according to AODV-GT is the one with the lowest cost DC_i. This route is the least possible route to be attacked and it introduces the lowest HIDS computational cost. This makes sense due to the fact that malicious nodes prefer to damage parts of eMANET which have high number of legitimate nodes achieving high utility.

Our future work involves experimenting with different areas, number of nodes and pause time. However, the most important aspect we have to take into account is the MAC layer protocol. Especially, we plan to use the IEEE 802.11n protocol which uses multiple-input multiple-output (MIMO) and channel-bonding/40 MHz operation to the physical layer and frame aggregation to the MAC layer. As a result the number of dropped packets due to link failures will be decreased significant.

Acknowledgment

The authors wish to acknowledge the support of the ICT European Research Programme and all their partners in PEACE: PDMF&C, Instituto de Telecomunicaes, FhG Fokus, University of Patras, Thales, Telefonica, CeBit.

References

[1] "Securing ad hoc networks in extreme emergency cases," *Proc. WWRF*, 2009.

[2] E. A. Panaousis, A. T. R. Ramrekha, K. Birkos, C. Papageorgiou, V. Talooki, G. Matthew, C. Nguyen, C. Sieux, C. Politis, T. Dagiuklas, and J. Rodriguez, "A framework supporting extreme emergency services," *ICT-MobileSummit*, 2009.

[3] J. Liu, F. Yu, C.-H. Lung, and H. Tang, "Optimal combined intrusion detection and biometric-based continuous authentication in high security mobile ad hoc networks," *IEEE Transactions on Wireless Communications*, vol. 8, no. 2, pp. 806–815, Feb. 2009.

[4] F. Anjum and P. Mouchtaris, *Security for Wireless Ad–hoc Networks*. John Wiley & Sons, 2006.

[5] A. Huhtonen, "Comparing aodv and olsr routing protocols," in *Seminar on Internetworking, Sjkulla*, 2004.

[6] T. A. Ramrekha and C. Politis, "An adaptive qos routing solution for manet based multimedia communications in emergency cases," in *ICST Mobilight*, Athens, Greece, 2009.

[7] M. Pietro and M. Refik, "Game theoretic analysis of security in mobile ad hoc networks," in *Research Report RR-02-070, Institut Eurecom*, Sophia-Antipolis, 2002.

[8] W. Yu and K. R. Liu, "Game theoretic analysis of cooperation stimulation and security in autonomous mobile ad hoc networks," *IEEE Transactions on Mobile Computing*, vol. 6, no. 5, pp. 507–521, 2007.

[9] M. Osborne and A. Rubinstein, *A Course in Game Theory*. The MIT Press, July 1994.

[10] A. Agah, K. Basu, and S. K. Das, "Security enforcement in wireless sensor networks: A framework based on non-cooperative games," *Pervasive and Mobile Computing*, vol. 2, no. 2, pp. 137–158, 2006.

[11] D. B. Johnson, D. A. Maltz, and J. Broch, "Dsr: The dynamic source routing protocol for multi-hop wireless ad hoc networks," in *In Ad Hoc Networking, edited by Charles E. Perkins, Chapter 5*. Addison-Wesley, 2001, pp. 139–172.

[12] C. Perkins and E. Royer, "Ad-hoc on-demand distance vector routing," in *Proceedings of the 2nd IEEE Workshop on Mobile Computing Systems and Applications*, 1997, pp. 90–100.

[13] N. Bulusu, D. Estrin, L. Girod, and J. Heidemann, "Scalable coordination for wireless sensor networks: Self-configuring localization systems," in *Proceedings of the Sixth International Symposium on Communication Theory and Applications*, 2001.

[14] I. D. Chakeres and C. E. Perkins, "Dynamic manet on-demand routing protocol, ietf internet draft, draft-ietf-manet-dymo-12.txt, february 2008."

[15] C. Papageorgiou, K. Birkos, T. Dagiuklas, and S. Kotsopoulos, "An obstacle-aware human mobility model for ad hoc networks," *17th IEEE/ACM International Symposium on Modelling, Analysis and Simulation of Computer and Telecommunication Systems (MASCOTS)*, September, 2009.

[16] [Online]. Available: http://www.wltl.ee.upatras.gr/humo/