ISSN : 2394-2975 (Online)
ISSN : 2394-6814 (Print)
Vol. 2, Issue 3 (July - Sept. 2015)
International Journal of Advanced Research in Education Technology (IJARET)

# Securing AODV from Blackhole Attacks in EMANETS by Using Non-Zero Game Theory

[I]P. Moulichandraobula Reddy, [II]B. Prabhakara Reddy
[I]M Tech, [II]Professor & HOD
[I,II]Dept of CSE, Bheema Institute of Technology & Science, Adoni, AP, India

**Abstract**
*A Mobile Ad hoc Network (MANET) is a self-configuring infrastructure less network of mobile devices connected by wireless channel. "Ad hoc" is a Latin word and it means "for this purpose". The MANETs are finding more likely importance due to their flexibility, ease and speed with which these networks can be deployed as well as reconfigured. This allows many excessive emergency cases such as forest fires or tube terrorist attacks, military battle field, natural disaster recovery and etc. We apply the term emergency Mobile Ad hoc Networks (EMANETS) which are deployed in emergency cases. The rescuers have difficulty using traditional legacy networks due to destruction or collapse of the infrastructure in such events. So the security is the main concern for these networks. 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 EMANETS. In this paper we propose a game theoretic approach called GTA-AODV (Game Theoretic approach-AODV) to provide defence against black hole attacks. GTA-AODV is based on the concept of non-cooperative non-zero game theory.GTA-AODV outperforms AODV in terms of malicious dropped packets when black hole nodes exist within the eMANETs. Our simulations were implemented using the network simulator ns-2.*

**Keywords**
*EMANETS, Black hole attack, AODV, Game Theory*

## I. Introduction

A MANET is a set of mobile nodes that can communicate with each other without the use of predefined infrastructure or centralized administration [1], [2]. The network nodes in a MANET, not only act as the ordinary network nodes but also as the routers for other peer devices to find out the shortest path to forward a packet and to perform basic networking functions like packet forwarding, routing without the need of an established infrastructure. All the nodes of an ad hoc network depend on each another in forwarding a packet from source to its destination, due to the limited transmission range of each mobile node's wireless transmissions. As nodes may be mobile, entering and leaving the network, the topology of the network will change continuously. Due to self-organize and rapidly deploy capability, MANETs are used with different applications including battlefield communications, urgent situation relief scenarios, law enforcement, virtual class room and etc. Currently, the secure routing is the hot topic in MANET research as it is essentially defenceless for several opponent attacks. 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 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 MANET, (iv) wireless data transmission does not make available clear line of defence, gateways and firewalls and (v) MANETs have constantly varying topology outstanding to the movement of nodes in and out of the network.

The network layer in MANET is predisposed to various attacks such as Black hole attacks, Wormhole attacks [3][4]. The disadvantage of the 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. Amongst these, we attempt in analyzing and improving the security of the routing protocol AODV [5] against the Black hole attacks. Black hole is one of the main attacks in MANET and is considered as the most common attack made against the AODV routing protocol. The black hole attack involves malicious node pretending to have the shortest and freshest route to the destination by constructing false sequence number [6] in control messages. The planning done by the black hole node will refuse the legitimate Route Reply (RREP) message from other nodes especially the reply message coming from the actual destination node. AODV protocol was created without any security considerations. Thus, no protection mechanism was built to detect the existence of malicious attack. We study various methods proposed to overcome the black hole attack in the AODV-based MANET. MANET security is usually

Based on encryption and authentication techniques. However, such schemes are not always sufficient due to insider attacks launched by compromised nodes. Since such risks cannot be completely eliminated there comes a need for intrusion detection systems (IDS) to defend MANETs [7] & [8]. 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. Nodes that are equipped with IDS sensors, operating in loose mode, can monitor the traffic sent or received by their neighbours in order to detect spiteful activities or deviation from predictable behaviours. It is worth mentioning here the concept of IDS. According to [7] 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 throughout operating system check logs.
- Network-based IDS (NIDS) which do not run on every host but on some areas called as clusters (9) within the MANET.

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

ISSN : 2394-2975 (Online)
ISSN : 2394-6814 (Print)

This paper is structured as follows. In section 2 we discuss about related work of MANET security with game theoretic considerations. In section 3 we introduce the concept of Game Theory. In section 4 the system model for a two player non – cooperative game in the context of MANET is discussed. In section 5 a new protocol called GTA-AODV is proposed to improve the security aspects of AODV against black hole attack. The simulation results are included in section 6 and concluded this paper in section 7. Finally our plans for future work are discussed in section 8.

## II. Related Work

Game theory has been used broadly in computer and communication networks to model a variety of problems. In the description, many schemes propose game theoretic solutions for intrusion detection or security provision within the area of MANETs. Bencsath et al. [10] applied game theory and client puzzles to devise a defence against denial of service (DoS) attacks. In the area of MANETs, Michiardi et al. [11] used cooperative and non-cooperative game theoretic constructs to develop a reputation based architecture for enforcing cooperation. Kodialam et al. [12] used a game theoretic framework to model intrusion detection via sampling in communications networks and developed sampling schemes that are optimal in the game theoretic setting. Few works propose game theoretic solutions for intrusion detection within the area of MANETs. The most important of them, according to our estimation are the [13-19]. To the best of our knowledge none of them propose a method of conniving the defending and attacking probability distributions over Mamet's nodes by maximizing the utility of the MANET and any malicious coalition at the NE. In the paper [13] 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. In addition, the [14] proposes a distributed mechanism which extends the generation of a cluster IDS model by electing different IDS leaders each time. In [15] authors have proposed a Bayesian game formulation to support intrusion detection in wireless ad hoc networks. In [16] authors use a dynamic Bayesian game framework to analyze the position between regular and malicious nodes in a MANET. Authors in [14] exploit ways to enforce cooperation in autonomous ad hoc networks when conditions of noisy and imperfect observation happen. The same authors in [19] they have examined the dynamic interactions between good nodes and adversaries in MANETs as secure routing and packet forwarding games. In [18] authors have used a game theoretic framework to examine secure cooperation stimulation in
Autonomous MANETs.

## III. Concept of Game Theory

The individual most closely related with the creation of the theory of games is John von Neumann, one of the greatest mathematicians of the 20th century. Von Neumann's work culminated in a fundamental book on game theory written in collaboration with Oskar Morgenstern entitled Theory of Games and Economic Behaviour, 1944. Game theory is a branch of applied mathematics that uses models to study interactions with formalized inducement structures games. It has applications in a variety of fields, including economics, international relations, evolutionary biology, political science, and military approach. In order to find the NE in a non-zero sum game we have to consider the concept of the dominant strategy.Game theory provides us with tools to study situations of conflict and cooperation. Such a situation exists when two or more decision makers who have different objectives act on the same system or share the same set of resources. Therefore, game theory is concerned with finding the best actions for individual decision makers in such situations and recognizing stable outcomes. Some of the assumptions that one makes while formulating a game are:

1. There are at least two players in a game and each player has, available to him/her, two or more well-specified choices or sequences of choices.
2. Each and every possible combination of plays available to the players leads to a well-defined end-state (win, loss, or draw) that terminates the game.
3. Associated with every possible outcome of the game is a collection of numerical payoffs, one to each player. These payoffs represent the value of the outcome to the different players.
4. All decision makers are rational; that is, each player, given two alternatives, will select the one that yields the greater payoff.

Game theory has been conventionally divided into cooperative game theory and non-cooperative game theory. The two branches of game theory are different in how they formalize interdependence among the players. In non-cooperative game theory, a game is a detailed model of all the moves available to the players. In contrast, cooperative game theory abstracts away from this level of detail and describes only the outcomes that result when the players come together in different combinations. In this paper, we consider non-cooperative non-zero game theory.

### 3.1. About Non-Cooperative Game Theory

Non-cooperative game theory studies situations in which a number of nodes/players are involved in
An interactive process, whose outcome is resolute by the node's individual decisions and, in turn, affects the well-being of each node in a possibly different way. Non-cooperative games can be classified into a few categories based on numerous criteria. Non-cooperative games can be classified as static or dynamic based on whether the moves made by the players are simultaneous or not. In a static game, players make their approach choices simultaneously, without the knowledge of what the other players are choosing. Static games are commonly represented diagrammatically using a game table that is called the normal form or strategic form of a game. In contrast, in a dynamic game, there is a strict order of play. Players take turns to create their moves, and they know the moves played by players who have gone before them. Game trees are used to illustrate dynamic games. This methodology is generally referred to as the extensive form of a game. A game tree illustrates all of the possible actions that can be taken by all of the players. It also indicates all of the possible outcomes at each step of the game. Non-cooperative games can also be classified as complete information games or incomplete information games, based on whether the players have complete or incomplete information about their adversaries in the game. Here information denotes the payoff-relevant kind of the adversaries. In a complete information game, each player has complete knowledge about his/her adversary's characteristics, approach spaces, payoff functions, and so on. For additional details on game theory, the reader is directed to [20], [21]. The fundamental elements of a game are the players, the actions, the payoffs and the information, known together as the rules of the game. A solution of a two-player game

is a pair of approaches that a rational pair of players might use. The solution that is most widely used for game theoretic problems is the Nash equilibrium (NE). At a NE, given the approaches of other players, no user can improve its efficiency level by making individual changes in its approach. Besides NE, other optimality criteria, such as Pareto optimality, Sub game accomplishment, Fairness, and Cheat proofing can be used to find the solution for game theoretic problems.

## IV. System Model

In this paper we think about game theory to model non-cooperative security games between a MANET, which is protected by IDS sensors operating at each node, and a set of collaborative malicious nodes called malicious coalition. Our work innovates by finding the secure and attack probability distributions, of any MANET and malicious coalition that maximize the effectiveness of the players at the Nash Equilibrium (NE) of a non-cooperative security game between the abovementioned players. These likelihood distributions represent the proportion of the computational attempt exhausted for defensive or attacking the nodes of a MANET. In other terms, this paper proposes a way to derive the intrusion detection or the attack attempt that a MANET or a malicious coalition, similarly, has to give in respect with their energy costs.

In terms of mathematics, let (B, V) be a game, where B is the bunch of strategy profiles and V is the set of payoff profiles. Let $b_{-i}$ be an approach profile of all players except for player i. When each player i Є {1... n} chooses the approach $b_i$ resulting in the approach profile $b = (b_1....b_n)$ then the player i obtain payoff or utility equal to $v_i(b)$. The utility depends on the approach chosen by player i as well as the approaches chosen by all the other players. A NE in an n-player game is a list of mixed approaches $b_1,\ldots,b_n$ an such that:

$$\mathbf{b_i \in \arg \max_{b_i \in B_i} v_i(b_i, b_{-i}) \ \forall i \in \{1,2,---,n\}} \quad (1)$$

In other words an approach profile b* Є B* is a Nash Equilibrium if no unilateral deviation in approach by any single player is profitable or:

$$\forall i, v_i(b_1^*, b_{-1}^*) \geq v_i(b_1^*, b_{-1}^*) \quad (2)$$

In our work, we propose a non-cooperative non-zero sum game theoretic approach. In game theory a zero sum game things to see a position 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 perception of the dominant approach. An approach is called dominant when it is better than any other approach for one player, no matter how that player's opponents could play. In terms of mathematics, for any player i, an approach b* Є B*i* dominate another approach b ' Є $B_{i\,if}$

$$v_i(b^*, b_{-1}) \geq v_i(b', b_{-i}) \quad (3)$$

Before going on to find NE, we appear in to the aspect whether NE exists for our game or not. The Nash-Theorem states that "Every game that has a finite approach form, with finite numbers of players and finite number of pure approaches for each player, has at least one NE involving pure or mixed approaches". We call an approach as a pure approach when a player chooses to take one action with probability 1. Mixed approach is an approach which chooses arbitrarily between possible moves. In other words this approach is a probability distribution over all the possible pure approach profiles. Since our non cooperative game has i). Finite strategic form. ii). Finite number of players (MANET and Malicious Coalition) iii). Finite number of pure strategies for each player (MANET: protecting & Non protective Malicious Coalition: attacking & non attacking). So the non cooperative game we scrutinize satisfy the needs of Nash theorem which means that there exists at least one NE in that game.

## V. Proposed Methodology

In this section, we define the emerging non-cooperative game between the MANET and potential black hole nodes and we describe our proposed tactic called GTA-AODV. 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. In addition, we describe the potential non-cooperative approaches of each player.

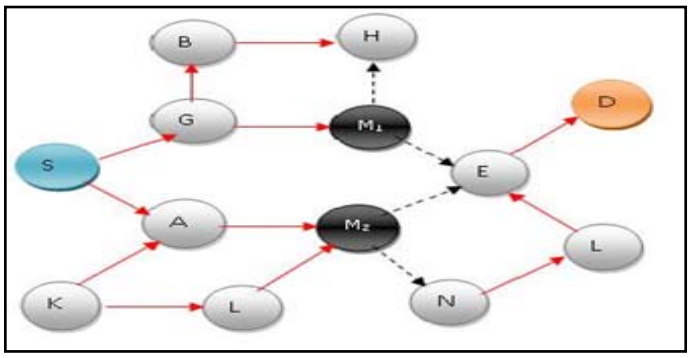


Fig.1 : A MANET where Black hole nodes damage the routing function by dropping packets

In figure 1 we explain a MANET scenario where two malicious nodes M1, M2 are trying to launch black hole attacks. Exclusively, the adversaries have the impending to advertise shorter routes to a destination node. As a consequence the source nodes consider that their packets should be passed through the nodes M1, M2. In this case, the function of the routing protocol has been disrupted. Afterward, the malicious nodes accomplish something in dropping an important number of packets.

In agreement with our tactic, we will formulate the described condition using a game theoretic frame. The players of the game are (i) the MANET and (ii) a black hole node. Thus, a two-player game is emerging. The game reaches a NE as we will explain later on. The perception could be pervasive for n black hole nodes assuming all the two-player games between the MANET and each malicious node. In our effort we scrutinize particularly the case of a non-cooperative game where the MANET tries to defend the most risky route among all the routes that are delivered to the source node by the AODV protocol. On the other dispense, malicious nodes try to launch black hole attacks on these routes. Towards the formulation of our game we depict the approach space for each player.

- Scheme space of the MANET:
  - Scheme 1($q_i$): the MANET protect a route i
  - Scheme 2($q_{-i}$): the MANET protect any other route −i.
- Scheme space of a blackhole node:
  - Scheme 1($h_i$): the blackhole node attacks a route i
  - Scheme 2($h_0$): the blackhole node does not attack MANET
  - --Scheme 2($h_L$): the blackhole node attacks a route L.

The payoff matrices of the MANET and Malicious nodes are revealed below in tables.

ISSN : 2394-2975 (Online)
ISSN : 2394-6814 (Print)

Table 1: Payoff Matrix of MANET & Malicious Nodes

| Scheme | $h_i$ | $h_0$ | $h_l$ |
|---|---|---|---|
| $q_i$ | $W_M(t) - PC_i$, $W_A(t) - AC_i$ | $W_M(t) - PC_i$, 0 | $W_M(t) - PC_i - FC_l$, $W_A(t) - AC_l$, for $l \neq i$ |
| $q_{-i}$ | $W_M(t) - PC_i - FC_i$ $W_A(t) - AC_i$ | $W_M(t) - PC_{-i}$, 0 | $W_M(t) - PC_{-i} - FC_l$, $W_A(t) - AC_l$, for $l \neq i$ -i |

In table 1, $W_M(t)$ is the utility of the MANET at time t, $PC_i$ is the cost of protecting a route i and $FC_i$ is the cost of failing to protect the route i. In adding together, we describe the number of one-hop neighbors of a node j as nnj. Especially, $PC_i$ depends on the values of nnj $\forall$ j $\in$ i and it is equal to:

$$\mathbf{PCi = \Sigma j \epsilon i\ nnj / \mathit{ni}} \quad (4)$$

Where is the number of nodes which constitute the route i. More in particular, the cost of protecting a route alongside a malicious node is essentially the cost of operating the HIDS sensors in the nodes which represent this route as well as in the one-hop neighbors of these nodes. The latter could hear the transmissions and they might contribute in the intrusion detection. Apparently, when a packet is forwarded through a route which has higher $PC_i$ value than another route, the cost for protecting the previous route is higher due to the contribution of more HIDS sensors. At the same time, according to equation (4) when $PC_i$ is minimized the number of nodes that a black hole 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 represent a route. The cost of failing to protect a route i is equal to the utility value that the attacker gains by plummeting packets on this route. A malicious node which communicates in a tiny region with a high number of genuine nodes has higher possibility to gain better effectiveness value by launching a black hole attack. In other words, when a route is comprised of nodes with undersized density, the black hole 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 [22], as follows:

$$\mathbf{\mathit{densj}\ (\mathit{R}) = NR\mathit{j}2\pi / \mathit{A}} \quad (5)$$

Where Rj is the radio transmission range of the node j, N is the number of nodes surrounded by the transmission range of node j at time t and A is the size of the region of the MANET. Therefore, we define:

$$\mathbf{\mathit{FCi} = \Sigma j \epsilon i\ \mathit{densj} / \mathit{ni}} \quad (6)$$

In maintenance with the concept of game formulation, the utility function of a malicious node is given in table 1. $AC_i$ is the cost of any attack against a route i and $W_A(t)$ is the proceeds of each thriving attack at time t.

It is worth mentioning why our game is a non-zero sum game. From the payoff matrices of the players we examine that even if the attacker does not attack the MANET is protecting. The payoff of the latter therefore decreases while the payoff of the malicious node is steady. The above assumption contradicts with the zero-sum statement which means that our game is a non-zero sum game. As we have mentioned in section 2, in this breed of games the NE has to be found considering the concept of the dominant approach.

### A. Mixed Strategy Nash Equilibrium

In the above payoff matrix the strategy $h_0$ of malicious node is dominated by the strategies $h_i$ and $h_l$. The dominated strategies are never used in Nash equilibrium i.e. finding its mixed strategy Nash equilibrium is equivalent to finding the mixed Nash equilibrium of the following game:

**Table 2:** Reduced payoff Matrix of MANET & Malicious nodes

| Scheme | $h_i$ | $h_l$ |
|---|---|---|
| $q_i$ | $W_M(t) - PC_i, W_a(t) - AC_i$ | $W_M(t) - PC_i - FC_l, W_a(t) - AC_l$, for $l \neq i$ |
| $q_{-i}$ | $W_M(t) - PC_{-i} - FC_i, W_a(t) - AC_i$ | $W_M(t) - PC_{-i} - FC_l, W_a(t) - AC_l$, for $l \neq i$ , -i |

Let we describe $P_d = (P_{s1}, P_{s2}..., P_{sn})$ as the defend probability distribution of MANET nodes in excess of N and $P_a = (p_{a1}, p_{a2}..., p_{an})$ as the attack probability distribution of Malicious nodes over N at mixed approach Nash Equilibrium. At mixed strategy Nash equilibrium both players should have some conventional payoffs from their two schemes;

Let we first consider the Mamet node i:

– If it plays with an approach or scheme $q_i$ then it will obtain a payoffs of $W_M(t) - PC_i$ with probability $P_{ai}$ and $W_M(t) - PC_i - FC_l$ with probability 1-$P_{ai}$.consequently its expected payoff E ($q_i$) from playing $q_i$ is

$$\mathbf{E(q_i) = (\mathit{W_M}(t) - PC_i)\ P_{ai} + (\mathit{W_M}(t) - PC_i - \mathit{FC_l})\ (1\text{-}P_a)} \quad (7)$$

– If it plays with an approach or scheme $q_{-i}$ then it will receive a payoffs of $W_M(t) - PC_{-i} - FC_i$ *with* probability $P_{ai}$ and $W_M(t) - PC_{-i} - FC_l$ *with* probability 1-$P_{ai}$.Consequently its predictable payoff E ($q_{-i}$) from playing $q_{-i}$ is

$$E(q_{-i}) = (W_M(t) - PC_{-i} - FC_i)\ P_{ai} + (W_M(t) - PC_{-i} - FC_l)\ (1\text{-}P_{ai}) \quad (8)$$

Mamet will mix the two strategies only when the predictable payoffs are same:

$$E(q_i) = E(q_{-i})$$
$$\Rightarrow (W_M(t) - PC_i)\ P_{ai} + (W_M(t) - PC_i - FC_l)\ (1\text{-}P_{ai}) = (W_M(t) - PC_{-i} - FC_i)\ P_{ai} + (W_M(t) - PC_{-i} - FC_l)\ (1\text{-}P_{ai})$$
$$\Rightarrow P_{ai} = (pc_i - pc_{-i}) / FC_i \text{ and } 1\text{-}P_{ai} = (pc_{-i} + FC_i - pc_i) / FC_i \quad (9)$$

Consequently the mixed strategy Nash equilibrium for player (Manet node) is:

$q_i$ with probability $(pc_i - pc_{-i}) / FC_i$ and $q_{-i}$ with probability $(pc_{-i} + FC_i - pc_i) / FC_i$,) i.e. the utility for the Manet at mixed strategy Nash equilibrium is given by

$$\mathbf{W_{manet} = (\mathit{W_M}(t) - PC_i)\ x\ (pc_i - pc_{-i}) / FC_i) + (\mathit{W_M}(t) - PC_{-i} - \mathit{FC_l})\ x\ (pc_{-i} + FC_i - pc_i) / FC_i)} \quad \mathbf{(\text{ or })}$$
$$\mathbf{(\mathit{W_M}(t) - PC_{-i} - FC_i)\ x\ (pc_i - pc_{-i}) / FC_i) + (\mathit{W_M}(t) - PC_{-i} - \mathit{FC_l})\ x\ (pc_{-i} + FC_i - pc_i) / FC_i,)} \quad (10)$$

Similarly we consider the malicious node:

– If it plays with an approach or strategy $h_i$ then it will receive a payoffs of $W_A(t) - ACi$ with probability Psi and $W_A(t) - AC_i$ with probability 1-$P_{si}$.Consequently its expected payoff E ($h_i$) from playing $h_i$ is

$$\mathbf{E\ (h_i) = (W_A\ (t) - AC_i)\ P_{si} + (W_A\ (t) - AC_i)\ (1\text{-}P_{si})} \quad \mathbf{(11)}$$

– If it plays with an approach or strategy $h_l$ then it will receive a payoffs of $W_A\ (t) - AC_l$ with probability $P_{si}$ and $W_A\ (t) - AC_l$ *with* probability $1\text{-}P_{si}$. Consequently its expected payoff E ($h_l$) from playing $h_l$ is

$$\mathbf{E\ (h_l) = (W_A\ (t) - AC_l)\ P_{si} + (W_A\ (t) - AC_l)\ (1\text{-}P_{si})} \quad \mathbf{(12)}$$

The malious node will mix the two strategies only when the predictable payoffs are same:
E ($h_i$) = E ($h_l$) ⇒) ($W_A$ (t) – $AC_i$) $P_{si}$ + ($W_A$ (t) – $AC_i$) (1-$P_{si}$ = ($W_A$ (t) – $AC_l$) $P_{si}$ + ($W_A$ (t) – $AC_l$) (1-$P_{si}$) But it is the game with saddle point i.e. min (max column) = max (min row) = 0. When the game has a saddle point then the payoff for the player is same irrespective of the strategy it plays. So there is no requiring combining the strategies to get the improved payoff. To facilitate is utility for the malicious coalition at mixed strategy Nash equilibrium is given by

$$\mathbf{W_{MC} = W_A\ (t) - AC_i = W_A\ (t) - AC_l} \quad \mathbf{(13)}$$

### B. Integrating GTA-AODV with AODV Protocol

The way how our new secure routing protocol GTA-AODV integrates in to AODV protocol is described here. We assume that a source node S wants to find out a route to a destination 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 $u_A = 1/nn_A$.

i) If A does not have a route to D it forwards the packet according to AODV.
ii) On the other hand, if A has a route to D, first it has to add its utility value $w_A$ to the utility value of the route A to D in order to derive the utility w AD. Second, A adds the value of w 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.
iii) 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.

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 GTA-AODV, 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). In the next step, S derives the average value $w_i$ *(ave)* of each route i which has cached using the following equation:

$$\mathbf{w_i(ave) = (nhops_i + 1) / \Sigma_{j \in i}\ nn_j} \quad (14)$$

The $nhops_i$ value indicates the number of hops which is included in the AODV packet. The number of hops is the only mutable information of the packet in the AODV packet. 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 calculation 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 successful route in terms of HIDS sensors computational cost surrounded by 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. The source node 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 wrecked, 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.

## VI. Simulation Results

The simulation effort is conceded out using the network simulator NS-2.35 (23) which so accepted amongst the explore groups to estimate the Mamet i.e. regular and malicious nodes varied approach Nash equilibrium.

### A. Simulation Setup

The proposed approach has been implemented on a discrete event network simulator as well as the simulations are accepted out in arbitrarily generated MANETs. The expected node can track its neighbors outgoing packets by neighbors monitoring. We simulated the areas which are equal to 600 meters (m) x 600(m) and 1000m x 1000m for the total simulation period of 2000 seconds. But in this credentials only the graphs for the simulation area 600 meters (m) x 600(m) are incorporated as there is a constraint in the number of papers. We used pause time equal to 20 seconds and the simulation is conceded out for the different node mobility speeds 2, 4, 6, 8, and 10 meters per seconds. We generated the both UDP and FTP traffic and we examined the cases of 20, 40, 60, 80, and 100 mobile

Nodes. One third of the nodes are simulated as the black hole nodes for each of the above scenarios, equally. Each simulation is repetitive 50 times and the average data are used as the final resu

It is merit mentioning that even if we do not have black hole nodes within MANET, a number of dropped packets leftovers due to failures of the wireless communications links. The situation becomes worst in our case due to the actuality that we implicit the reality of obstacles. The latter introduce higher impenetrability in the rescue 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 means the number of dropped packets is decreased though it cannot reach the case without malicious nodes. This occurs due to the fact that an HIDS need some time before reacting to an attack. Evidently, this is the time to notice this attack. In adding together, depending on the thresholds which have been set at the HIDS sensors for the uncovering of the attacks, there is diverse extent of straightforwardness in recognizing the malicious activities.

### B. Simulation Results

In figures 2 and 3 the variations in packet delay is shown with respect to number of nodes and different mobility speeds of nodes as a comparison for alleged AODV protocol and our new GTA-AODV protocol. In figure 4 and 5 we illustrate how the AODV protocol and our GTA-AODV protocol generate Packet delivery Ratio (PDR) with respect to number of nodes and different mobility of nodes respectively. In figures 6 and 7 we depicted the

ISSN : 2394-2975 (Online)
ISSN : 2394-6814 (Print)

Dropped Packets for AODV protocol and our new GTA-AODV protocol with respect to number of nodes and different mobility speeds of nodes respectively.

### FTP Traffic

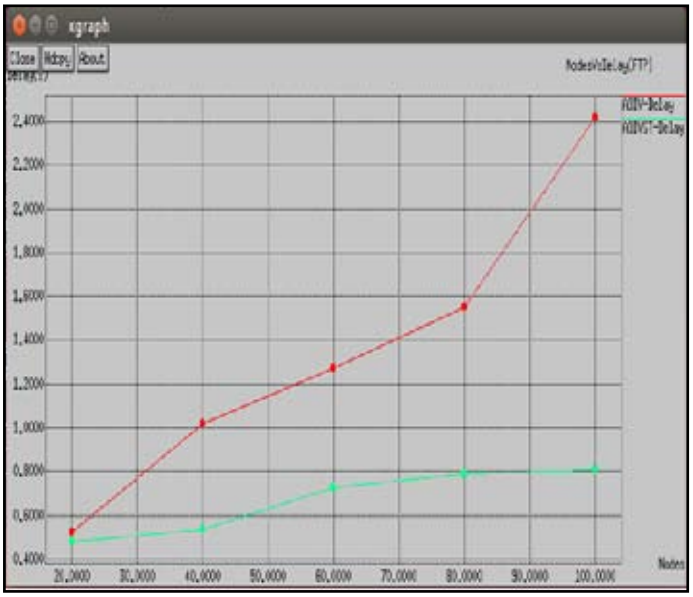


Fig 2: MANET Nodes Vs Packet Delay

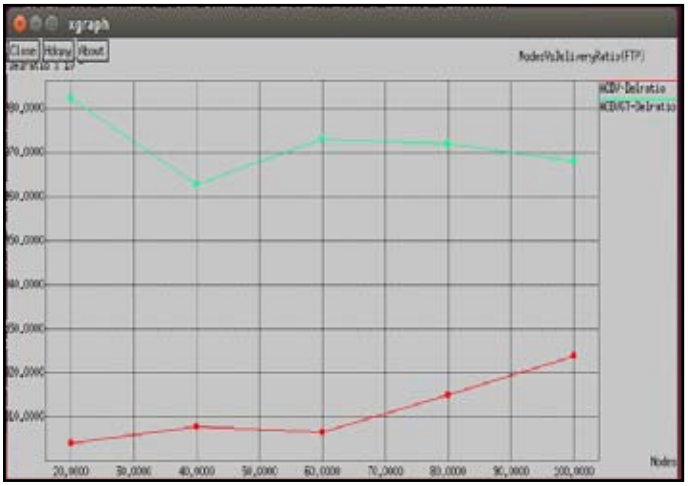


Fig 3: MANET Nodes Vs Packet Delivery Ratio

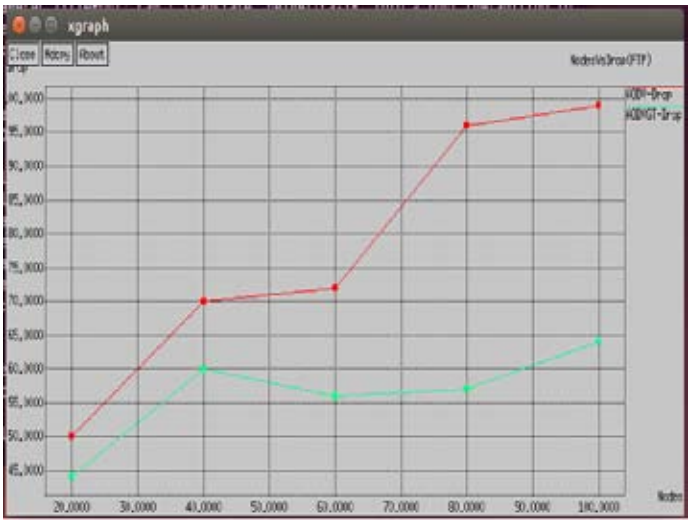


Fig 4: MANET Nodes Vs Packet Drop

### UDP Traffic

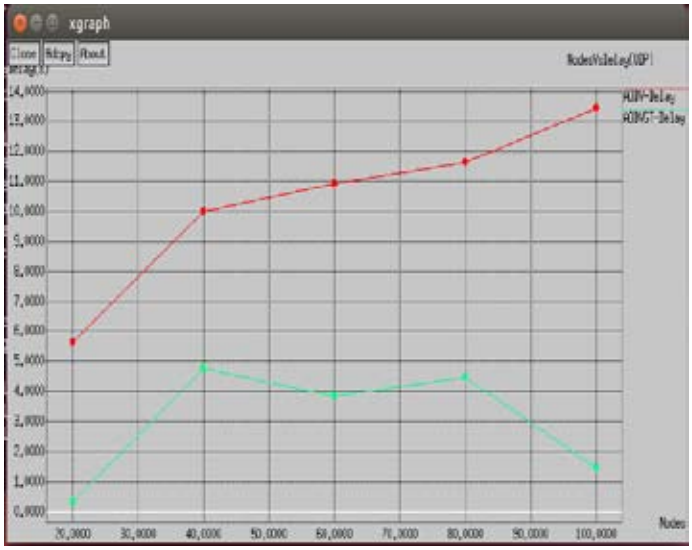


Fig 5: MANET Nodes Vs Packet Delay

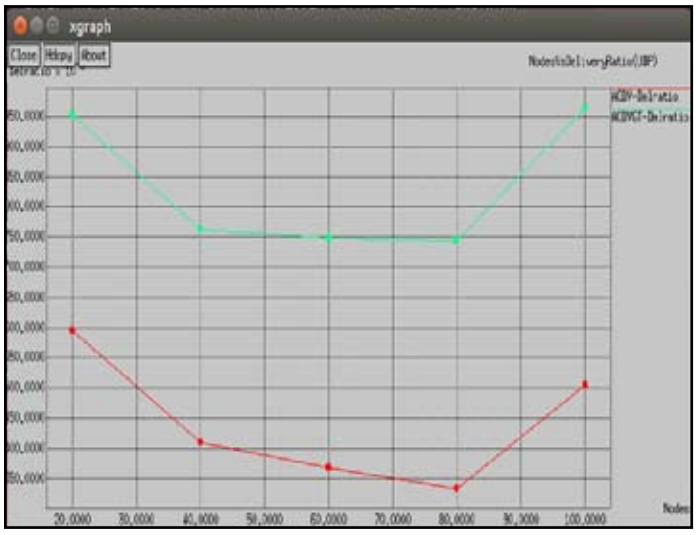


**Fig 6:** MANET Nodes Vs Packet Delivery Ratio

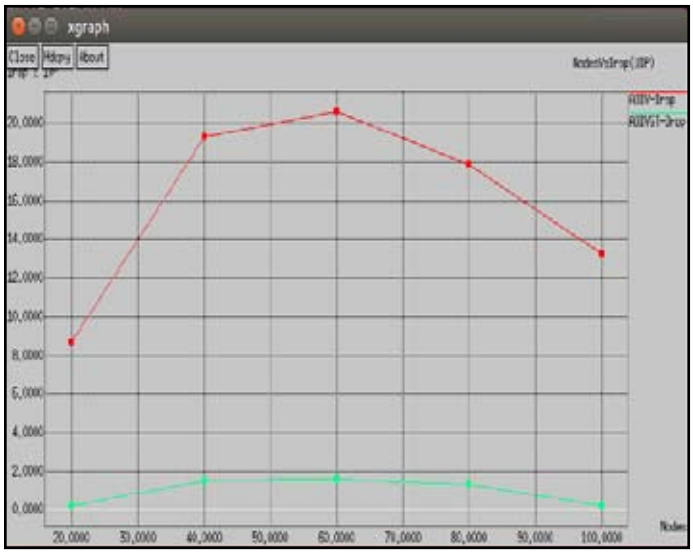


**Fig 7:** MANET Nodes Vs Packet Drop

### VII. Conclusion

We proposed a game theoretic approach called GTA-AODV by incorporating security aspects into the AODV protocol to conquer

the attacks from Black hole nodes. The simulation results show that GTA-AODV outperforms AODV in terms of Packet Delivery Ratio and Packet Delay for different number of black hole nodes and mobility speeds of MANET nodes. We furthermore supposed Host based Intrusion Detection System (HIDS) sensors which are able to perceive the malicious nodes and exclusive of them from the MANET. The extent of this work though is not to explain the function of HIDS but to propose the GTA-AODV approach as it was described expansively in this paper.

To this end, we formulated a game between the MANET and each potential black hole node. We showed that the most successful route to forward the packets according to GTA-AODV is the one with the lowest cost DCi. This route is the slightest 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 MANET which have high number of genuine nodes achieving high utility.

Our simulation results proved that our proposed GTA-AODV protocol outperforms the reputed AODV protocol by enhancing the average packet delivery ratio (PDR) .The simulation results also showed that the proposed GTA-AODV is achieved the outstanding performance in terms of dropped packets and the delay of the packets compared to the AODV protocol.

## VIII. Future Work

Our future work involves the procedures to experiment with cluster heads instead of operating HIDS sensors at every node in the MANET for reducing the cost of defending route PCi and subsequently attractive the payoff function of the Mobile ad hoc network. That is looking for the different potential to replace the existing HIDS approach with NIDS approaches. Also the simulation may be conceded out for different MANET areas, number of nodes, mobility speeds and traffics.

## References

[1] *E. A. Panaousis and C. Politis, "Securing ad hoc networks in extreme emergency cases," in WWRF, Paris, France, 2009.*

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

[3] *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*

[4] *Tanu Preet Singh, Satinder Kaur and Vikrant Das "Security Threats in Mobile Adhoc Network: A Review" in IRACST – IJCNWC, ISSN: 2250-3501 Vol. 2, No. 1, 2012*

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

[6] *M. J. Osborne and A. Rubinstein, A Course in Game Theory. Cambridge, MA: The MIT Press, 1994.*

[7] *R.Divya, N.Saravanan, "Authentication and Intrusion Detection System for Mobile Ad-Hoc Networks" International Journal of Innovative Research in Computer and Communication Engineering, Vol.2, Special Issue 1, March 2014*

[8] *Payal N. Raj, Prashant B. Swadas" DPRAODV: A Dyanamic Learning System against Blackhole Attack in AODV Based Manet." arXiv: 0909.2371,2009.*

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

[10] *Ming-Yang Su," Prevention of selective black hole attacks on mobile ad hoc networks throug intrusion detection systems", Elsevier, Computer Communications 34 (2011) 107–117*

[11] *H. Deng, Wei Li, and D. P. Agrawal, "Routing Security in Wireless Ad Hoc Network," IEEE Communications Magzine, vol. 40, no. 10, October 2002.*

[12] *"A Review Paper on Ad Hoc Network Security",Karan Singh, Rama Shankar Yadav and Ranvijay,International Journal of Computer Science and Security,Vol.1:Issue(1) [2008]*

[13] *M.Parsons and P.Ebinger, "Performance Evaluation of the Impact of Attacks on mobile ad hoc networks".*

[14] *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.*

[15] *M. Kodialam and T. V. Lakshman, "Detecting net-work intrusions via sampling: A game theoretic ap- proach," in IEEE INFOCOMM 2003, pp. 1880–1889, Piscataway, NJ, USA, Apr.2003.*

[16] *C. Kruegel and T. Toth, "Flexible, mobile agent based intrusion detection for dynamic networks," Technical Report TUV-1841-2002-27, Distributed Systems Group at the Technical University of Vi-enna, 3rd Floor, Central Entrance, 1040 Vienna, Austria, Apr. 30 2002.*

[17] *F Richard Yu, Helen Tang, Shengrong Bu and , Du Zheng "Security and quality of service (QoS) co-design in cooperative mobile ad hoc networks", EURASIP Journal on Wireless Communications and Networking (Springer open access journal),2013.*

[18] *B. Bencsath, I. Vajda, and L. Buttyan, "A game based analysis of the client puzzle approach to defend against dos attacks," in Proceedings of the IEEE Conference STCN - 2003, pp. 763-767*

[19] *P. Michiardi and R. Molva, "Core: A collaborative reputation mechanism to enforce node co- operation in mobile ad hoc networks," in Proceedings of the 6th IFIP CMS Conference, September 2002.*

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

[21] *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.*

[ 22] *A.E. Roth, The Shapley Value: Essays in Honor of Lloyd S.Shapley, Cambridge University Press, 1988.*

[23] *http://www.nsnam.com/*

ISSN : 2394-2975 (Online)
ISSN : 2394-6814 (Print)

**Author's Profile**

*Palagati Moulichandraobula Reddy B.Tech degree in Information Technology in the year 2013 from JNTU Anantapur. Currently his pursuing M.Tech in Computer Science & Engineering from JNTU Anantapur.His Research and area of interest is Mobile Ad hoc Networks.*

*Prabhakara Reddy Baggidi received B.Tech degree in Electronics and Communication Engineering in the year 1997 from SV University, Tirupathi, India. He is awarded with M-Tech degree in Digital Systems & Computer Electronics in the year 2002 and currently carrying out Ph.D work in association with Jawaharlal Nehru Technological University, Anantapur, India. He guided many academic projects for the last 15 years of teaching experience. His research interests are in the field of Mobile Ad hoc Networks and Optical Networks.*