# DEFENDING BLACKHOLE ATTACKS IN MOBILE AD HOC NETWORKS USING NON-ZERO GAME THEORY

B. Prabhakara Reddy[1], M.N. Giri Prasad[2]
Associate Professor[1], Professor & HOD[2]
[1]Dept of ECE, Bheema Institute of Technology & Science, Adoni, AP, India
[2]Dept of ECE, JNTUA College of Engineering, Anantapur, AP, India

***ABSTRACT***

*Mobile ad hoc networks (MANETs) are an infrastructure less self configuring networks of mobile devices connected by an open access wireless links. 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 the use of this kind of networks in special circumstances, such as military battle field, natural disaster recovery and emergency medical services and etc. As MANETs lack a centralized infrastructure, they are exposed to a lot of attacks such as blackhole attack, wormhole attack and etc. So the security is the main concern for these networks. Especially secure routing is important given the fact that potential attackers aim to disrupt the appropriate operation of the routing protocol within a MANET. In this paper we propose an ad hoc routing protocol called GTASA (Game theoretic approach to secure AODV) protocol to defend MANET against blackhole attacks. GTASA is based on the concept of non-cooperative non-zero game theory and it outperforms AODV in terms of malicious dropped packets when blackhole nodes exist within the MANET. Our simulations were implemented by means of the popular network simulator NS-2.*

***KEYWORDS:*** *Blackhole attack, Malicious, GTASA, AODV, Game Theory.*

## I. INTRODUCTION

A MANET is a collection 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 optimal path to forward a packet. 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, emergency relief scenarios, law enforcement, virtual class room and etc. There are 15 major issues and sub-issues involve in MANET such as routing, multicasting/broadcasting, security, location service, clustering, mobility management, TCP/UDP, IP addressing, multiple access, radio interface, bandwidth management, power management, fault tolerance, QoS/multimedia and standards/products.

Currently, the secure routing is the hot topic in MANET research as it is inherently vulnerable for several adversary 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 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.

The network layer in MANET is susceptible to various attacks viz. Denial-of-service (DoS) attacks such as Black hole attacks, Wormhole attacks, Sinkhole attacks, eavesdropping with a malicious intent, spoofing the control and/or data packets transacted and the malicious modification/alteration of

the packet contents [3]&[4]. 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. 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 many attacks that take place in MANET and is considered as one of the most common attacks 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 manipulation done by the blackhole node will deny the genuine 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 or captured 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 promiscuous mode, can monitor the traffic sent or received by their neighbours in order to detect malicious activities or deviation from conventional 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 through operating system audit logs
- Network-based IDS (NIDS) which do not run on each host but on some areas called as clusters (9) 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 initiated automatically in order to stop the attack.

This paper is organized as follows. In section 2 we discuss related work within the realm 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 GTASA is proposed to enhance 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 extensively in computer and communication networks to model a variety of problems. In the literature, many schemes propose game theoretic solutions for intrusion detection or security provision within the realm of MANETs. Bencsath *et al.* [10] applied game theory and client puzzles to devise a defense 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 or security provision within the realm of MANETs. The most important of them, according to our opinion are the [13], [14], [15], [16], [17], [18] and [19]. To the best of our knowledge none of them propose a method of calculating the shielding and attacking probability distributions over Manet's nodes by maximizing the utility of the MANET and any malicious coalition at the NE. In the paper [13] authors have modeled the interactions between a host-based IDS and an attacker as a basic signaling 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 lifetime 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 situation 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. GAME THEORY

The individual most closely associated 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 Behavior, 1944. Game theory is a branch of applied mathematics that uses models to study interactions with formalized incentive structures ("games"). It has applications in a variety of fields, including economics, international relations, evolutionary biology, political science, and military approach. 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. 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 each 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 traditionally divided into cooperative game theory and non-cooperative game theory. The two branches of game theory differ 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 games.

## 3.1. 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 determined 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 several 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 generally 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 make their moves, and they know the moves played by players who have gone before them. Game trees are used to depict 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 characteristics 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 further details on game theory, the reader is directed to [20], [21].

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 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 utility level by making individual changes in its approach. Besides NE, other optimality criteria, such as Pareto optimality, Sub game perfection, Fairness, and Cheat proofing can be used to find the solution for game theoretic problems.

## IV. SYSTEM MODEL

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 maximize the utility of the players at the Nash Equilibrium (NE) of a non-cooperative security game between the aforementioned players. These probability distributions represent the percentage of the computational effort spent for shielding 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, has to give in respect with their energy costs.

In terms of mathematics, let (A, P) be a game, where A is the set of approach profiles and P is the set of payoff profiles. Let $a_{-i}$ be an approach profile of all players except for player i. When each player i Є {1... n} chooses the approach $a_i$ resulting in the approach profile a = ($a_1$... $a_n$) then the player i obtain payoff or utility equal to $p_i$ (a). 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 $a_1$,..., $a_n$ such that:

$$a_i \in \arg \max_{a_i \in A_i} p_i(a, a_{-i}) \forall i \in \{1, 2, .., n\} \quad (1)$$

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

$$\forall i, p_i(a_i^*, a_{-i}^*) \geq p_i(a_i, a_{-i}^*) \quad (2)$$

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 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 $a^*$ Є $A_i$ dominate another approach a ' Є $A_{i\ if}$

$$p_i(a^*, a_{-i}) \geq p_i(a', a_{-i}) \quad (3)$$

Before proceeding to find NE, we look in to the aspect whether NE exist 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 randomly 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: Shielding & Non shielding Malicious Coalition: attacking & non attacking). So the non cooperative game we examine satisfies the requirements 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 blackhole nodes and we describe our proposed methodology called GTASA. 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 approaches of each player.

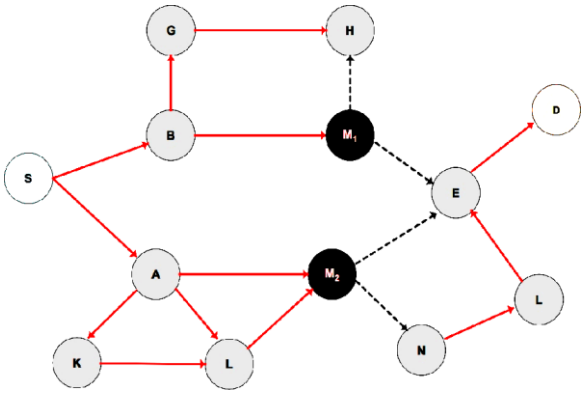


**Fig.1.** A MANET where Blackhole nodes damage the routing function by dropping packets

In figure 1 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. In our work we examine especially the case of a non-cooperative game where the MANET tries to defend the most critical route among all the routes that are delivered to the source node by the AODV protocol. On the other hand, malicious nodes try to launch blackhole attacks on these routes. Towards the formulation of our game we define the approach space for each player.

- approach space of the MANET:
  - Approach 1($s_i$): the MANET shield a route i
  - Approach 2 ($s_{-i}$): the MANET shield any other route −i.
- approach space of a blackhole node:
  - Approach 1($b_i$): the blackhole node attacks a route i
  - Approach 2($b_0$): the blackhole node does not attack MANET
  - -- Approach 2($b_K$): the blackhole node attacks a route K.

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

**Table 1:** Payoff Matrix of MANET & Malicious Nodes

| Approach | $b_i$ | $b_o$ | $b_k$ |
|---|---|---|---|
| $s_i$ | $U_M(t) - SC_i$, $U_A(t) - AC_i$ | $U_M(t) - SC_i$ , $0$ | $U_M(t) - SC_i - FC_k$ , $U_A(t) - AC_k$ , for $k \neq i$ |

| | | | |
|---|---|---|---|
| $s_{-i}$ | $U_M(t) - SC_{-i} - FC_i$ , $U_A(t) - AC_i$ | $U_M(t) - SC_{-i}$ , *0* | $U_M(t) - SC_{-i} - FC_k$ , $U_A(t) - AC_k$ *for* $k \neq i$ , *-i* |

In table 1, $U_M(t)$ is the utility of the MANET at time t, $SC_i$ is the cost of shielding a route i and $FC_i$ is the cost of failing to shield the route i. In addition, we define the number of one-hop neighbors of a node j as $nn_j$. Especially, $SC_i$ depends on the values of $nn_j$ $\forall j \in i$ and it is equal to:

$$\mathbf{SC_i = \Sigma_{j\epsilon i}\, nn_j / n_i} \quad \textbf{(4)}$$

Where $n_i$ is the number of nodes which constitute the route i. More precisely, the cost of shielding 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 $SC_i$ value than another route, the cost for shielding the former route is higher due to the participation of more HIDS sensors. At the same time, according to equation (4) when $SC_i$ 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 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 [22], as follows:

$$\mathbf{dens_j\,(R) = NR_j^2 \pi / A} \quad \textbf{(5)}$$

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 S is the size of the region of the MANET. Therefore, we define:

$$\mathbf{FC_i = \Sigma_{j\epsilon i}\, dens_j / n_i} \quad \textbf{(6)}$$

In keeping 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 $U_A$ (t) is the profit of each successful 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 observe that even if the attacker does not attack the MANET is shielding. 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 2, in this kind of games the NE has to be found considering the concept of the dominant approach.

## 5.1. Mixed Strategy Nash Equilibrium

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

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

| Approach | $b_i$ | $b_k$ |
|---|---|---|
| $s_i$ | $U_M(t) - SC_i$ , $U_a(t) - AC_i$ | $U_M(t) - SC_i - FC_k$ , $U_a(t) - AC_k$ , for $k \neq i$ |

| | | |
|---|---|---|
| $s_{-i}$ | $U_M(t) - SC_{-i} - FC_i$ , $U_a(t) - AC_i$ | $U_M(t) - SC_{-i} - FC_k$ , $U_a(t) - AC_k$ *for* $k \neq i$ , $-i$ |

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

Let we first consider the Manet node i:

– If it plays with an approach or strategy $s_i$ then it will receive a payoffs of $U_M(t) - SC_i$ with probability $P_{ai}$ and $U_M(t) - SC_i - FC_k$ with probability $1\text{-}P_{ai}$.Therefore its expected payoff E ($s_i$) from playing $s_i$ is

$$\mathbf{E(s_i) = (U_M(t) - SC_i)\, Pai + (U_M(t) - SC_i - FC_k)\,(1\text{-}P_{ai})} \quad (7)$$

– If it plays with an approach or strategy $s_{-i}$ then it will receive a payoffs of $U_M(t) - SC_{-i} - FC_i$ *with* probability $P_{ai}$ and $U_M(t) - SC_{-i} - FC_k$ *with* probability $1\text{-}P_{ai}$.Therefore its expected payoff E ($s_{-i}$) from playing $s_{-i}$ is

$$\mathbf{E(s_{-i}) = (U_M(t) - SC_{-i} - FC_i)\, Pai + (U_M(t) - SC_{-i} - FC_k)\,(1\text{-}P_{ai})} \quad (8)$$

Manet will mix the two strategies only when the expected payoffs are same:

$E(s_i) = E(s_i) \Rightarrow (U_M(t) - SC_i)\, Pai + (U_M(t) - SC_i - FC_k)\,(1\text{-}P_{ai}) = (U_M(t) - SC_{-i} - FC_i)\, Pai + (U_M(t) - SC_{-i} - FC_k)\,(1\text{-}P_{ai})$

$$\Rightarrow \mathbf{Pai = (sc_i - sc_{-i}) / FC_i \quad and\ 1\text{-}Pai = (sc_{-i} + FC_i - sc_i) / FC_i} \quad (9)$$

Therefore the mixed strategy Nash equilibrium for player (Manet node) is: $s_i$ with probability $(sc_i - sc_{-i}) / FC_i$ and $s_{-i}$ with probability $(sc_{-i} + FC_i - sc_i) / FC_i$,) i.e. the utility for the Manet at mixed strategy Nash equilibrium is given by

$$\mathbf{U_{manet} = (U_M(t) - SC_i) \times (sc_i - sc_{-i}) / FC_i) + (U_M(t) - SC_{-i} - FC_k) \times (sc_{-i} + FC_i - sc_i) / FC_i)}$$

**( or )**

$$\mathbf{(U_M(t) - SC_{-i} - FC_i) \times (sc_i - sc_{-i}) / FC_i) + (U_M(t) - SC_{-i} - FC_k) \times (sc_{-i} + FC_i - sc_i) / FC_i,)} \quad (10)$$

Similarly we consider the malicious node:

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

$$\mathbf{E(b_i) = (U_A(t) - AC_i)\, P_{si} + (U_A(t) - AC_i)\,(1\text{-}P_{si})} \quad (11)$$

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

$$\mathbf{E(b_k) = (U_A(t) - AC_k)\, P_{si} + (U_A(t) - AC_k)\,(1\text{-}P_{si})} \quad (12)$$

The malious node will mix the two strategies only when the expected payoffs are same:

$E(b_i) = E(b_k) \Rightarrow (U_A(t) - AC_i)\, P_{si} + (U_A(t) - AC_i)\,(1\text{-}P_{si}) = (U_A(t) - AC_k)\, P_{si} + (U_A(t) - AC_k)\,(1\text{-}P_{si})$

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 need to mix up the strategies to get the better payoff. That is utility for the malicious coalition at mixed strategy Nash equilibrium is given by

$$\mathbf{U_{MC} = U_A(t) - AC_i = U_A(t) - AC_k} \quad (13)$$

## 5.1. Integrating GTASA with AODV Protocol

The way how our new secure routing protocol GTASA 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 $u_A$ to the utility value of the route A to 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.

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 GTASA, 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 $u_i$ *(ave)* of each route i which has cached using the following equation:

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

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 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. 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 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.

## VI. SIMULATION RESULTS

The simulation work is carried out using the network simulator NS-2.34 (23) which so popular among the research groups to evaluate the Manet i.e. regular and malicious nodes mixed strategy Nash equilibria.

### 6.1. Simulation Setup

The proposed strategy has been implemented on a discrete event network simulator and the simulations are carried out in randomly generated MANETs. The regular 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 documentation only the graphs for the simulation area 600 meters (m) x 600(m) are included as there is a constraint in the number of papers. We used pause time equal to 20 seconds and the simulation is carried out for the different node mobility speeds 2, 4, 6, 8, and 10 meters per seconds. We generated the both UDP and TCP traffic and we examined the cases of 50, 60, 70, 80, 90 and 100 mobile nodes. One third of the nodes are simulated as the blackhole nodes for each of the above scenarios, correspondingly. Each simulation is repeated 50 times and the average data are used as the final result.

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 cannot 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 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.

## 6.2. Simulation Results

In figures 2 and 3 the variations in packet delivery ratio (PDR) is shown with respect to number of nodes and different mobility speeds of nodes as a comparison chart for reputed AODV protocol and our new GTASA protocol. In figure 4 and 5 we show how the AOD protocol and our GTASA protocol generates control over head with respect to number of nodes and different mobility of nodes respectively. In figures 6 and 7 we depicted the Normalized routing overheads for AODV protocol and our new GTASA protocol with respect to number of nodes and different mobility speeds of nodes respectively.

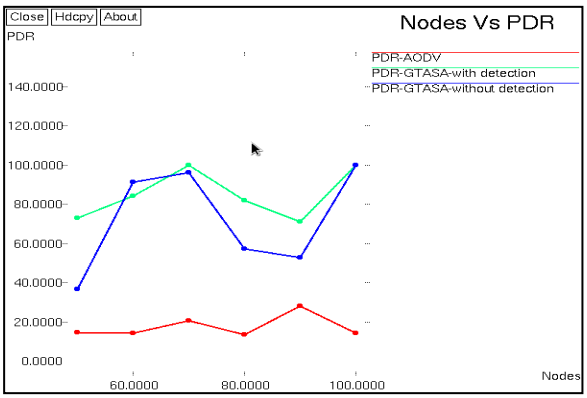


**Fig2.** Packet Delivery Ratio Vs Number of MANET nodes

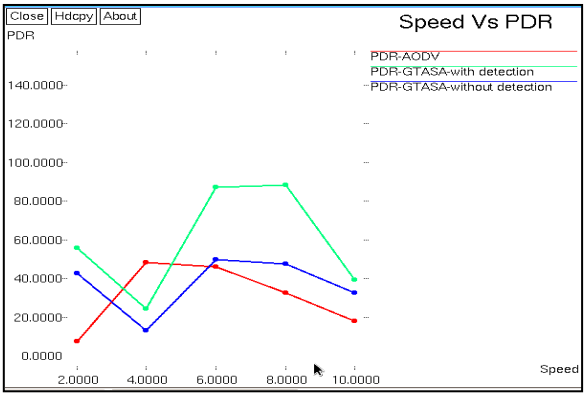


**Fig3**. Packet Delivery Ratio Vs speed of MANET nodes

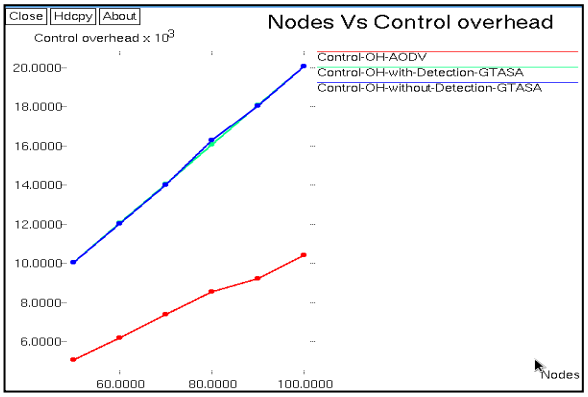


**Fig 4.**Contol overhead Vs Number of MANET nodes

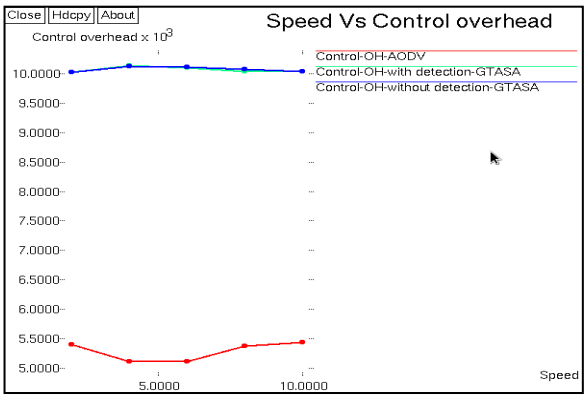


**Fig 5.**Contol overhead Vs speed of MANET nodes

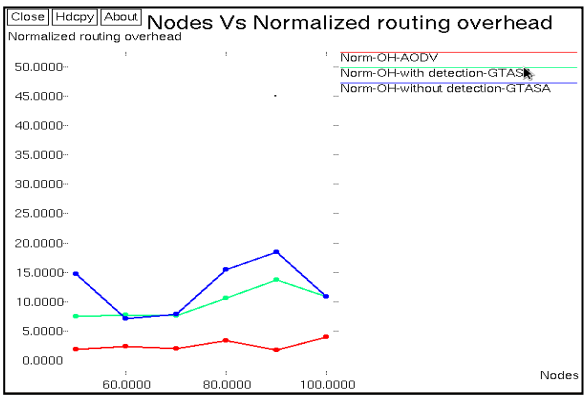


**Fig 6.** Normalized routing overhead Vs Number of MANET nodes

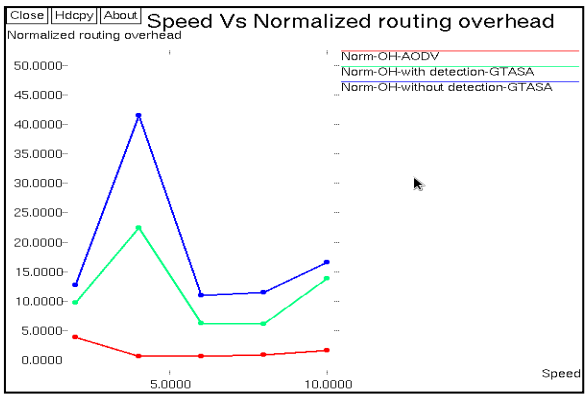


**Fig 7.**Normalized routing overhead Vs speed of MANET nodes

For both the traffics GTASA outperforms AODV by yielding better PDR as shown in graphs. But the security aspects of our proposed GTASA protocol are achieved at the expense of increase in Control

overhead but fortunately the normalized routing overhead is for better in our GTASA protocol.

## VII. CONCLUSION

We proposed a game theoretic approach called GTASA by incorporating security aspects into the AODV protocol to overcome the attacks from Black hole nodes. The simulation results show that GTASA outperforms AODV in terms of Packet Delivery Ratio and Normalized routing overhead for different number of black hole nodes and mobility speeds of MANET nodes. We additionally supposed Host based Intrusion Detection System (HIDS) sensors which are able to detect the malicious nodes and excluding them from the MANET. The scope of this work however is not to explain the function of HIDS but to propose the GTASA approach as it was described extensively in this paper.

To this end, we formulated a game between the MANET and each potential blackhole node. We showed that the most effective route to forward the packets according to GTASA 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 MANET which have high number of legitimate nodes achieving high utility.

Our simulation results proved that our proposed GTASA protocol outperforms the reputed AODV protocol by enhancing the average packet delivery ratio (PDR) from 20% to more than 60%. The simulation results also showed that the proposed GTASA is achieved this just at an expense of a nominal rise in Normalized routing overhead as 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 shielding route $SC_i$ and consequently enhancing the payoff function of the Mobile ad hoc network. That is looking for the different possibilities to replace the existing HIDS approach with NIDS approaches. Also the simulation may be carried out for different MANET areas, number of nodes, mobility speeds and traffics.

## REFERENCES

[1] DharamVir, Dr. S.K. Agarwal, Dr. S.A.Imam, "Performance Analysis of MANET with Low Bandwidth Estimation", International Journal of Scientific and Research Publications, Volume 3, Issue 3, March 2013.

[2] 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

[3] Sudhir Agarwal, Sanjeev Jain, Sanjeev Sharma "A Survey of Routing Attacks and Security Measures in Mobile Ad hoc Networks", JOURNAL OF COMPUTING, Volume 3, Issue 1, Jan 2011, ISSN 2151-9617.

[4] Ms.Supriya and Mrs.Manju Khari "Manet Security Breaches: Threat to A Secure Communication Platform" IJANS, Vol. 2, No. 2, April 2012.

[5] G. Jose Moses, Sunil Kumar, Prof.P.Suresh Varma and N.Supriya "A Simulation Based Study of AODV, DSR, DSDV Routing Protocols in MANET Using NS-2", IJARCSSE, Volume 2, Issue 3, March 2012.

[6] SUSHIL KUMAR CHAMOLI, SANTOSH KUMAR "Performance of AODV against Black Hole Attacks in Mobile ad hoc Networks "Int.J.Computer Technology & Applications, Vol 3 (4), 1395-1399.

[7] U. Sharmila Begam, Dr. G. Muruga Bhupathi "A recent secure intrusion detection system for Manets", ICISC-2013, Volume 3, Special Issue 1, January 2013.

[8] Emmanouil A. PANAOUSIS and Christos POLITIS "Non-Cooperative Games Between Legitimate Nodes and Malicious Coalitions in MANETs" Future Network and Mobile Summit 2011 Conference Proceedings.

[9] 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.

[10] 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

[11] 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.

[12] M. Kodialam and T. V. Lakshman, "Detecting network intrusions via sampling: A game theoretic approach," in *Proceedings of the 22nd IEEE INFOCOMM 2003*.
[13] 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.
[14] H. Otrok, N. Mohammed, L. Wang, M. Debbabi, and P. Bhattacharya, "A gametheoretic intrusion detection model for mobile ad hoc networks," Comp. Comm.,vol. 31, no. 4, pp. 708 – 721, 2008.
[15] Z. Ji, 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, 2010.
[16] 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.
[17] 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.
[18] W. Yu and K. Liu, "Game theoretic analysis of cooperation stimulation and security in autonomous mobile ad hoc networks," IEEE Trans. Mobile Compute., vol. 6, pp. 507 –521, May 2007.
[19] 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.
[20] D. Fudenberg and J. Tirole, Game Theory. Cambridge, MA: The MIT Press, 2002.
[21] M. J. Osborne and A. Rubinstein, A Course in Game Theory. Cambridge, MA: The MIT Press, 1994.
[22] N. Nisan, T. Roughgarden, E. Tardos, and V. V. Vazirani, Algorithmic Game Theory. New York, USA: Cambridge University Press, 2007.
[23] www.isi.edu/nsnam/ns/tutorial/.

## AUTHOR

**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.

**M. N. Giri Prasad** is currently working as Professor and HOD, Dept. of ECE, JNTUA, Andhra Pradesh, India. He received B.Tech degree from JNTU College of Engineering, Anantapur, Andhra Pradesh, India in 1982, M.Tech degree from Sri Venkateshwara University, Tirupathi, Andhra Pradesh, India in 1994 and Ph.D. degree from J.N.T University, Hyderabad, Andhra Pradesh, India in 2003. He is having 85 National and International publications to his credit. He is the member of IE(India), Member of ISTE, and NAFEN. His areas of research are Signal & Image Processing, Microcontroller Applications, and Embedded Systems.