# A Game Theoretic Approach for Protecting AODV from Blackhole Attacks in EMANETs

P. Moulichandraobula Reddy[1], B. Prabhakara Reddy[2]
M Tech[1], Associate Professor[2]
Dept of CSE, Bheema Institute of Technology & Science, Adoni, AP, India[1&2]

## Abstract:

*A Mobile Ad Hoc Network (MANETs) are an innovative wireless networking standards for mobile hosts. Unlike traditional mobile wireless networks, MANETs do not rely on any fixed infrastructure. Instead, they rely on each other to continue the network connected. The MANETs are finding more liable importance due to their flexibility, ease and speed with which these networks can be deployed as well as reconfigured. The military vigilant and security sensitive operations are still the main applications of MANET and also we find a trend to implement for commercial uses due to their unique properties. We concern the term emergency Mobile Ad hoc Networks (EMANETs) which are deployed in emergency cases. The nature of MANETs makes them appropriate to be utilized in the context of an extreme emergency for all rescue operational teams. But, secure routing in MANET is critical as there has been the absence of central authority, and the other reasons such as thwart tampering, scarcity of wireless links, dynamic topology and resource constraints come into the picture. Especially secure routing is important given the fact that potential attackers aim to disrupt the appropriate operation of the routing protocol within an EMANETs. So the security is the main anxiety for these networks. In this paper we propose a game theoretic approach called GTA-AODV (Game Theoretic approach-AODV) to provide defense against black hole attacks. Based on different performance parameters like PDR, throughput, end-to-end delay, packet drop, normalized overhead. 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:** *GTA-AODV, EMANETs, AODV, Game Theory, Black hole attack*

## 1. Introduction

In this paper we are paying attention on how to provide security to MANET beside attacks and how to stay away from them. The majority of the effort has been done before in this field focused on the routing procedure and how it is been pretentious by the intruders or attackers[1],[2],[3],[4]. We do not disagree with the intention of security and routing processes are dissimilar, other than in our move toward we will seem to be even at the routing procedure as of a security perception. In this epoch of expertise every technical domain are constantly grown-up and extend. The confirmation of this expansion is dissimilar kinds of communication devices is general for all persons. As the field of communication is developed require to afford elevated concert end to end consistent liberation is increases. At the for a moment security procedures is a one of the majority imperative concern in communication arrangement.

This paper describes on implementing game theoretic approach called GTA-AODV (Game Theoretic Approach-AODV) and we combine this into the reactive Ad hoc On-demand Distance Vector (AODV) routing protocol to give defense against black hole attacks. GTA-AODV is based on the concept of non-cooperative game theory. GTA-AODV outperforms AODV in terms of malicious dropped packets when black hole nodes are present inside the EMANETs against Black hole attack on Reactive Routing protocol, On Demand Distance Vector (AODV) in Mobile Ad Hoc Network. The security of the AODV protocol is compromised by a particular type of attack called 'black hole' attack. In this attack a malicious node advertises itself as having the shortest path to the node whose packets it wants to interrupt. The black hole problem in MANETs is a critical security difficulty specified the fact that one or more malicious nodes use the routing protocol to announce them as having the shortest path to the node whose packets they want to intercept. The range of this thesis is to revise the effects of Black hole attack and how much is the impact of the attack over On Demand Distance Vector (AODV). For that purpose, we did the relative analysis of AODV protocol with normal AODV nodes, black hole nodes in a network and also along with IDS nodes (which can prevent the black hole attack) in the existence of black hole nodes based on Performance measures (PDR, End-to-End delay, throughput, Normalized Overhead) by creating scenarios varying the number of nodes, seed values and mobility of nodes using Network Simulator 2 (NS2) tool. Ultimately the result shows the performance measures of Normal AODV, Black hole AODV.A MANET is a set of mobile nodes that can communicate with each other without the use of predefined infrastructure or centralized administration [5], [6]. The network nodes in a MANET, not only act as the normal network nodes but also as the routers for other peer devices to find out the shortest path to forward the-

  

packet and to perform basic networking functions like packet forwarding, routing without the required 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.

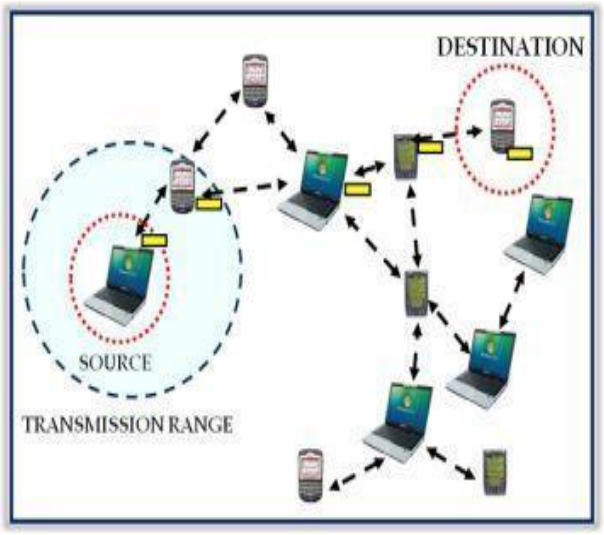


Fig 1: A Structure of Mobile Ad hoc Networks

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 defenseless 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 [7][8]. 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 [7] 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 [9],[10] in control messages. The planning done by the black hole node will refuse 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. Conversely, such schemes are not always sufficient due to insider attacks launched by compromised nodes.

This paper is prepared as follows. In section 2 we discuss about related work of MANET security with game theoretic considerations. In section 3 we introduce the proposed methodology. In section 4 the simulation results are included and in section 5 concluded this paper. Finally our plans for future work are discussed in section 6.

## 2. Background

In this paper the exertion is associated to AODV and GTA-AODV protocols and to offer the security for the MANET. Routing is an essential function of any MANET given the aspect that the nodes participate the function of routers. Subsequently, the implementation of routing protocols is indispensable requirement though we need guaranteeing that these protocols are secure. We use also the proactive Optimized Link State Routing (OLSR) protocol or the reactive AODV routing protocol. The selection of these two protocols is based on the study published in which shows that OLSR and AODV are the most striking for an adaptive solution for multimedia transmission. The protocol is considered to acclimatize its routing actions according to the size of an EMANET. The drawback of the most ratified routing protocols for MANETs is the fact that they have been developed without considering security mechanisms in progress. The container becomes more decisive when tremendous emergency communications must be deployed at the ground of a rescue. In these cases adversaries could launch dissimilar sort of attacks negative the quality of the communications.

### i) Black hole Attack:

Black hole attack is a type of Denial-of-Service (DoS) attack consummate by dropping packets. We demonstrate a case where two malicious nodes launch black hole attacks ensuing to drop packets within the MANET. Subsequent to the initiation of a black hole 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 black hole 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 table5, it is the first node that responds to the Route Request (RREQ) by sending a Route Reply (RREP) to the source node.

  

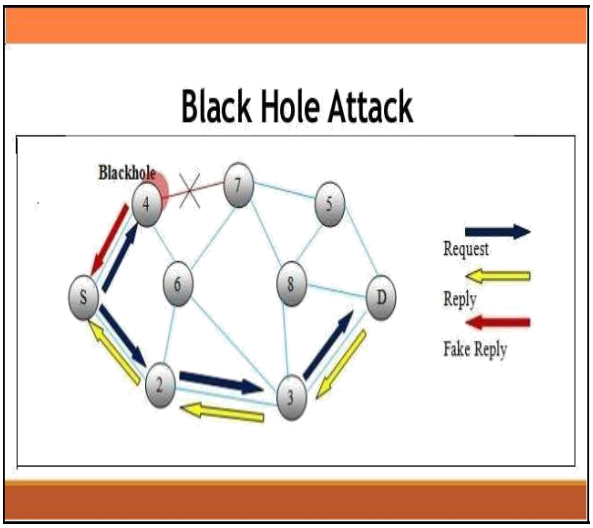


Fig 2: A Blackhole Attack in MANETs

## ii) Game Theory:

Game theory is a branch of applied mathematics that uses models to study relations with formalized incentive structures games. It has applications in a assortment of fields, with economics, international relations, evolutionary biology, political science, and military approach. Game theory provides us with tools to study situations of variance 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. So, game theory is disturbed with finding the best actions for individual decision makers in such situations and recognizing stable outcomes. Some of the assumptions that one makes as formulating a game are: There are at least two players in a game and each player has, accessible to him/her, two or more well-specified choices or sequences of choices. Each achievable mixture of plays available to the players leads to a well-defined end-state (win, loss, or draw) that terminates the game. Related by every probable result of the game is a set of numerical payoffs, one to each player. These payoffs stand for the rate of the outcome to the unlike players. All decision makers are realistic; that is, each player, given two alternatives, will choose the one that yields the greater payoff. Game theory has been traditionally separated into cooperative game theory and non-cooperative game theory. The two branches of game theory differ in how they formalize interdependence between the players. In non-cooperative game theory, a game is a complete model of all the moves available to the players. In compare, cooperative game theory abstracts away from this stage of aspect and describes only the outcomes that result when the players come together in different combinations.

In this paper, on-cooperative game theory studies situations in which a number of nodes/players are concerned in an interactive process whose effect is resolute by the node's individual decisions and, in turn, affects the well-being of each node in a perhaps different way. Non-cooperative games can be classified into a few categories based on some criteria. Non-cooperative games can be classified as static or dynamic based on whether the moves through by the players are synchronized or not. In a static game, players create their loom choices concurrently, lacking the knowledge of what the other players are choosing. Static games are normally represented diagrammatically with a game table that is called the usual form or strategic form of a game. It also indicates all of the possible outcomes at every 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. Now information denotes the payoff-relevant kind of the adversaries. In difference, in a dynamic game, there is a strict order of play [11],[12],[13],[14]. Players get turns to create their moves, and they recognize the moves played by players who have left before them. A game tree illustrates all of the possible actions that can be engaged by all of the players. In a complete information game, each player has complete knowledge about his/her the vital elements of a game are the players, the activities, the payoffs and the information, known jointly as the rules of the game. An answer of a two-player game is a pair of approaches that a sensible pair of players might use. The key that is most broadly used for game theoretic problems is the Nash equilibrium (NE). At a NE, precise the approaches of previous players, no user can get better its efficacy level by creation individual changes in its approach.

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 unlike 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.

Non-cooperative game theory studies situations in which a number of nodes/players are involved in an interactive process, whose outcome resolute by the node's individual decisions and, in turn, affects the

  

well-being of each node in a possibly different way. 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 unfinished information games, based on whether the players have complete or incomplete information about their adversaries in the game. On-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. A game tree illustrates all of the possible actions that can be taken by all of the players. 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. This methodology is generally referred to as the extensive form of a 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).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 [15], [16]. 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.

## 3. Proposed System

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. In this paper we propose a game theoretic approach called GTA-AODV (Game Theoretic Approach-AODV) and integrate this into the reactive Ad hoc On-demand Distance Vector (AODV) routing protocol to provide defence against black hole attacks. The concept of non-cooperative game theory is the main anxiety to apply GTA-AODV. The GTA-AODV outperforms AODV in terms of malicious dropped packets when black hole nodes exist within the EMANET. In this work we propose a methodology, for securing the reactive Ad hoc On-demand Distance Vector (AODV) routing protocol, called GTA-AODV. Moreover, GTA-AODV decreases the probabilities of the prospective 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 Through almost all destination.

the emerging two-player game between the EMANET and each of the black hole nodes converges to a Nash Equilibrium (NE) point when GTA-AODV is applied. In our work we examine especially the case of a non-cooperative game anywhere the MANET tries to defend the most crucial. Route between all the routes that are delivered to the source node by the AODV protocol. On the other hand, malicious nodes try to launch black hole attacks on these routes. AODV-GT improves the ratio of dropped for each received packets optimizing the computational cost. In this we are implementing the security mechanisms by using NS-2 simulator and note down the performance parameters like Delay and packet delivery ratio, throughput of the routing protocols of AODV and GTA-AODV.

## 4. Performance Analysis

This metrics accustomed to assess the effectiveness regarding project are usually PDR (Packet Delivery Ratio), End-to-End delay, Throughput, Number of packets drop. We learn about these kinds of metrics in depth.

**PDR (Packet Delivery Ratio):**

Packet delivery ratio pertains to the proportion regarding information packets received through the destination to that generated through the sources.

Mathematically, the idea can be explained as: PDR= S1÷ S2

Wherever, S1 can be the sum of the information packets received through the each and every destination and S2 can be the sum of the information packets generated through the each and every source.

**Average end-to-end packet delay:**

The normal time it will take for data packet to achieve the particular destination. Including almost all achievable delays a result of buffering while in route discovery latency, queuing on the program line. This kind of metric can be calculated through subtracting time when first packet has been sent through source through time when first data packet came to destination.

Mathematically, the idea can be explained as: Avg. EED=S/N

Where S can be the sum of the enough time expended to deliver packets for destination, and Nis the quantity of packets received through the destination nodes.

**Throughput:**

This pertains to the total variety of packets delivered in the entire simulation time. This throughput contrast implies that a few algorithms effectiveness margins are very shut under traffic insert regarding 50 and 100 nodes within MANET situation and still have huge margins any time variety of nodes boosts to help 200. Mathematically, the idea can be explained as:

Throughput= N/1000

Where N can be the quantity of bits received efficiently.

  

**Normalized routing overhead:**

The amount of command and information transmissions done through the protocol for each delivered data packet. This kind of metric measures the overall work that the protocol expends with the distribution of each data packet. For example, multicast efficiency regarding 5 shows that the protocol can make 5 packet transmissions on average for every data packet that's delivered to multicast receiver.

## 5. Simulation Results

In this section we preserve survive attentive of simulation and numerous use metrics instructed to scrutinize the success concerning project. Intended for you to state the Blackhole beat, we create with the summary of efficiency metrics for example PDR (Packet Delivery Ratio), End-to-End delay, Packet Drop, Throughput. These matrices are exceedingly imperative owing to its effectiveness evaluating network. Here the simulation results are shown in the graphs.

### 5.1. Simulation Details

The numbers of nodes we have regarded 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 result. 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.

### 5.2. Simulation Parameters

This test evaluates the suggested plan are actually completed while using the network simulator ns-2. This simulation statistics can be revealed within table. Effectiveness of the a few practices is usually looked at: (i) AODV protocol, (ii) Blackhole node with AODV protocol, (iii) GTA-AODV protocol i.e., Game theoretic approach based AODV protocol. Subsequent metrics are usually selected to evaluate and prevent the particular impression regarding Blackhole strike on the simulated network: (i) Packet delivery ratio (ii) Throughput (iii) End-to-End delay (iv) Number of Packet drop. This selected parameters intended for simulation are usually offered within pursuing table.

### 5.3. Simulation Results

In figures 3 and 7 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. 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 Anticipated for simulation are as a rule 10 to help 100 mobile nodes within the terrain part of 1000m * 1000m. All around 10% of them being opponents are typically supposed, which might be accomplishing information modify beat. We have additionally practical a number of UDP (User Datagram Protocol) cable connections with packet length 1024 bytes to assist copy traffic in the network. Each and every node at home repeats this definite conduct and capability to go can be different through responsibility each and every node motionless for a period of temporarily pause time. The proposed approach has been implemented on a discrete event network simulator as well as the simulations are accepted out in arbitrarily generated MANETs. 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 graphs for Number of nodes and the mobility. The Dropped Packets for AODV protocol and our new GTA-AODV protocol with respect to number of nodes and different mobility speeds of nodes respectively.

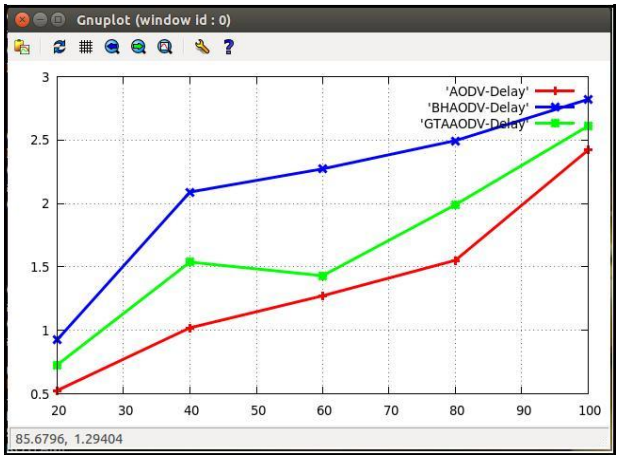


Fig 3: Nodes Vs Delay

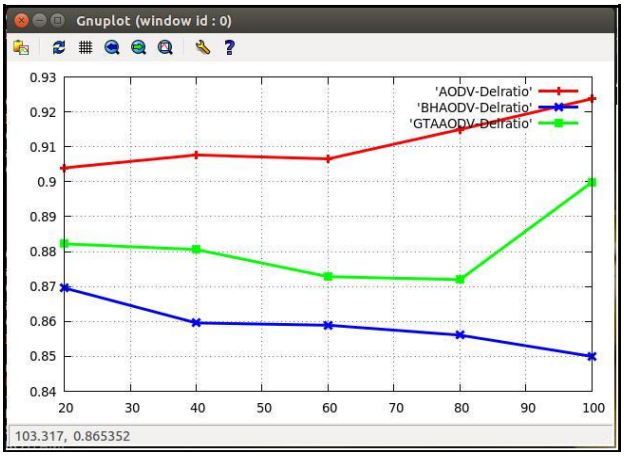


Fig 4: Nodes Vs Packet Delivery Ratio

  

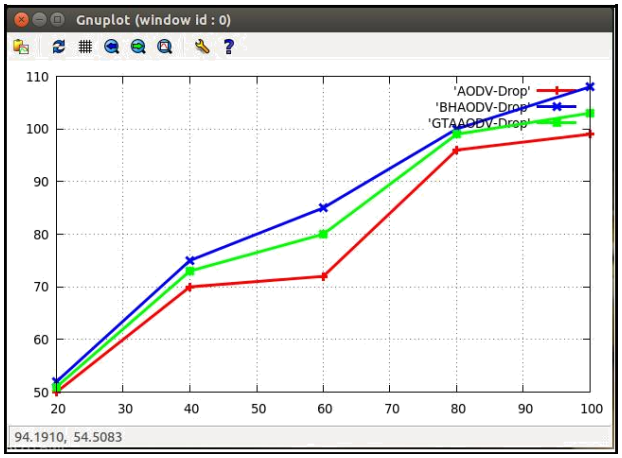


Fig 5: Nodes Vs Drop

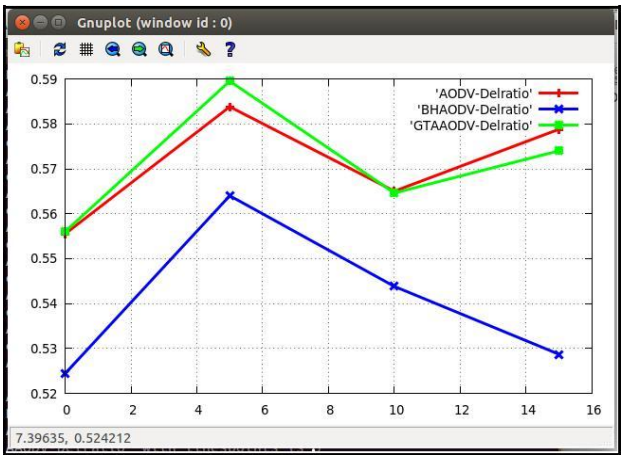


Fig 8: Mobility Vs Packet Delivery Ratio

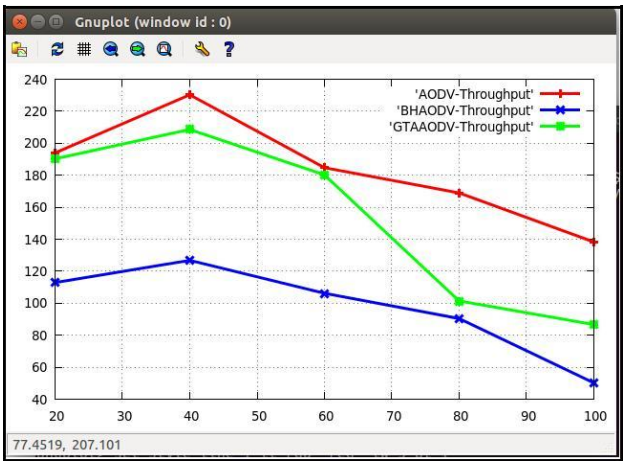


Fig 6: Nodes Vs Throughput

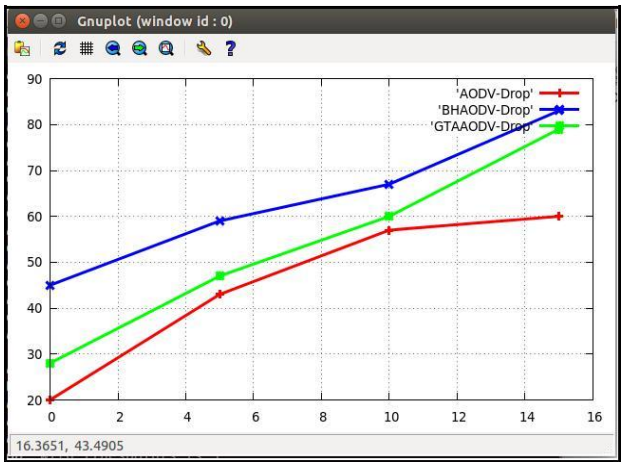


Fig 9: Mobility Vs Number of Dropped Packet

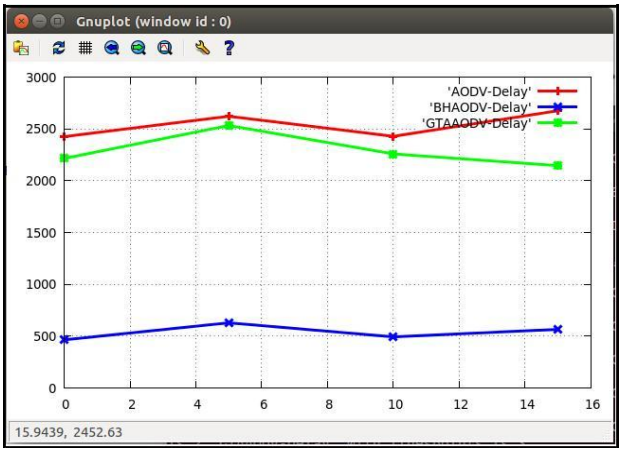


Fig 7: Mobility Vs Delay

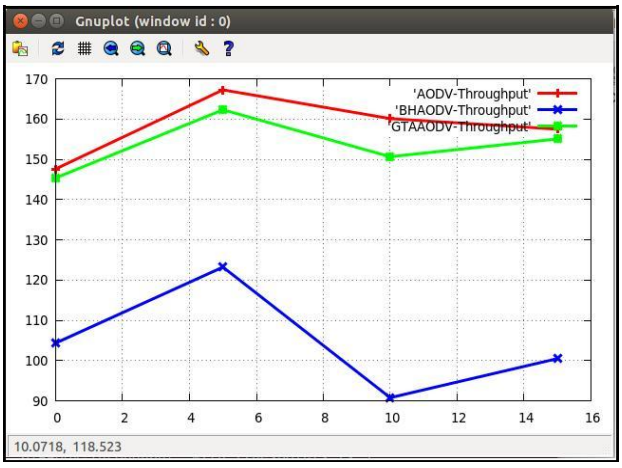


Fig 10: Mobility Vs Throughput

  

## 6. Conclusion

With this document, the challenge regarding Blackhole attack and its effects on the AODV routing protocol has been mentioned. Several techniques to get over this challenge have been suggested. This route discovery procedure inside the AODV can prone to Blackhole attack, it is therefore critical, a great effective safety measures is implemented in to the AODV protocol so that you can reduce the issues induced. We proposed a game theoretic approach called GTA-AODV by incorporating security aspects into the AODV protocol to conquer that GTA-AODV outperforms AODV in terms of Packet Delay and Packet Delivery Ratio, Number of dropped packets, throughput for different number of black hole nodes and mobility speeds of MANET nodes. 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. Therefore carried out an answer within simulation with a number of cases which in turn compresses the consequence regarding Blackhole nodes. 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 DeLay, Packet delivery ratio, Number of dropped packets and Throughput compared to the AODV protocol.

## 7. Future Exertion

Our future work involves experimenting with different areas, Number of nodes and pause time. We have investigated the issues regarding blackhole attack within mobile Ad hoc networks. Within our customer survey we have applied the particular AODV project although various other practices they can double to examine the results in the future. Distinct practices present various results. Which means greatest course-plotting project intended for minimizing the blackhole attack could possibly be determined. However diagnosis regarding Blackhole node can be one more future work. Within our work we experimented with to help discover and get rid of the Blackhole effect. There's also other kinds intended for removing the particular Blackhole effect based on the type of cable connections often TCP or perhaps UDP.

## References


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

*[2]"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]*

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

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

*[5]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.*

*[6]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*

*[7] 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*

*[8] 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.*

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

*[10]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*

*[11] Payal N. Raj, Prashant B. Swadas" DPRAODV: A DyanamicLearning System against BlackholeAttack in AODV Based Manet." arXiv: 0909.2371,2009.*

*[12] 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.*

*[13] 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*

*[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 INFOCOMM2003, pp. 1880–1889, Piscataway, NJ, USA, Apr.2003.*

*[16] C. Kruegel and T. Toth, "Flexible, mobile agent based intrusion detection for dynamic networks,"*

*[17] Technical Report TUV-1841-2002-27, Distributed Systems Group at the Technical University of Vienna, 3rd Floor, Central Entrance, 1040 Vienna, Austria, Apr. 30 2002.*


  

*[18] 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.*

*[19] 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*

## 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.*

  