A Survey of Selfish Node attack detection in Mobile Ad hoc Network (MANET)

[1]**K.Sudhaakar,** [2]**Dr.K.T.Meena Abarna,** [3]**Dr. EMohan,** [4]**Dr. T.Suresh**

[1] Research scholar, Department of Computer Science and Engineering, Annamalai University, Chidambaram, India, sudhaakarkumar@gmail.com
[2]Assistant Professor, Department of Computer Science and Engineering, Annamalai University, Chidambaram, India, abarnakt@yahoo.com
[3]Professor, Department of Computer Science and Engineering, Prince Shri Venkateshwara Padmavathy Engineering College, Chennai, India, emohan1971@gmail.com
[4]Associate Professor, Department of Computer Science and Engineering, Annamalai University, Chidambaram, India, sureshaucse@gmail.com

***Abstract*:** A network connecting mobile nodes wirelessly is known as MANET. In MANET the communication takes place with the help of mobile nodes. Using the wireless connection, mobile devices are connected and the nodes freely move where it wants to share information with each other. MANET's are dynamic in nature and do not have fixed infrastructure to control nodes in the networks. Wireless ad hoc networks has various characteristics like dynamic topology, limited resources, absence of central controller etc. Every node in a MANET forwards data so that it can reach to its destination. . All nodes are involved in packet forwarding in order to cooperate with each node. Suppose, if the nodes are not transferring the packets to its neighbor nodes it is called as selfish nodes. Considering all the features of MANET, nodes in MANET work on the principle of co-operating with other nodes in network to help in various activities of the network like successful transfer data from source to destination. Some nodes in the network take advantage of co-operation and pretend to be co-operating with other nodes however they are saving on their resources like battery and drop the data whenever they receive it without sending it to the required destination or intermediate nodes to the destination. Route discovery and packets forwarding consumes bandwidth and energy. A kind of routing misbehavior of node is few nodes may be act as selfish by taking part in finding route and upkeep process, but deny forwarding the packet. Such type of misbehavior reduce packet transfer ratio and also degrade system performance in terms of power and bandwidth. MANETs is lack in centralized monitoring and infrastructure less behavior makes it more vulnerable to attack, and difficult to detect selfish node effectively. The selfish node behavior presence leads to partition the network and makes an negative impact in the operation of the network.

Keywords: MANETs, Game Theoretical Approach, Supervisory Game,, IDSM, Selfish node.

I. INTRODUCTION

Architecture of Mobile ad hoc Network The mobile ad hoc network having more than one wireless mobile node and has the capability to transferring data to one another without help from a centralized administrator. Every device acts as end system and router in ad hoc network.

The network topology in a mobile ad hoc network is dynamic due to the integration of the nodes transiting with time because of the movement of nodes admission of new nodes and flight of nodes. From this, productive routing protocols are important for these nodes to communicate is shown in Fig. 1.

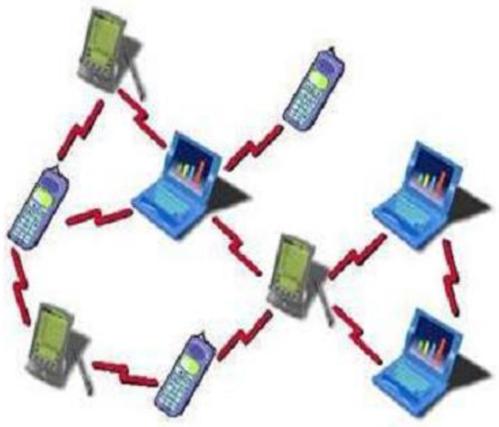


Fig. 1. Architecture of Mobile Ad hoc network

MANETs are basically p2p, multi-hop mobile networks in which collection of autonomous nodes cooperatively share with each other without having any fixed infrastructure [4]. MANETs plays a dominant role in many application areas such as disaster management, battle field operations, tactical situations, collaborative and distributed computing [5]. In this network, nodes can directly interacting with each other only when they are located within their transmission range, otherwise cooperation of intermediate nodes are expected to forward packets between senders and receivers in the network. Hence, the cooperation of intermediate nodes is very important for successful communication. Node that denies to forward packets is referred to as 'a selfish node'. Such selfish nodes do not cooperate to the basic network functions such as authorization, packet sending and routing in order to reduce battery power and bandwidth usage. They affect the altogether behavior of the network. Moreover, a node can also misbehave by dropping received packets or altering the packets to perform malicious attacks in the network which could reduce the packet delivery rates and again performance degradation will be the result.

The current patterns in wireless technology show that the dependency of masses on wireless devices have increased tremendously over the years. These devices work with wireless networks which are categorized into two types: infrastructure and infrastructure less networks. [6] Infrastructure networks consists of access points which act as a point of contact between the wired network and the wireless device. Networks present at our homes, hospitals, offices etc. comes under the category of networks discussed above. The later type of networks do not consist of access points and are not fixed infrastructure networks rather they are called ad hoc networks. These networks are dynamic in nature i.e. they can be constructed anytime and anywhere, they can easily communicate with any device directly through wireless medium without the need of any access point connectivity. Mobile ad-hoc network comes under this category. [6][1]

MANET is made up of independent wireless nodes or devices capable of sharing with other nodes via wireless links. These nodes are wireless and free to move in any direction, the topology of the network takes dynamic shape and hence no other device like router can be included in such networks to assist in routing activities for smooth data transfer. As a conclusion, nodes are multi-tasking and play role of both host and router in such networks, they do not rely on any fixed base station and lack in central controlling device, as a result node must manage among themselves for proper behavior of the network. Nodes can impart with the nodes available in its direct communication range, also nodes can send data to the other nodes which are out of its communication range by taking help of the intermediate nodes that are present on the path from source to destination [6][1]. An ad hoc wireless (MANET) is a self-organizing system of mobility stations attached by wireless links to form a network. There exists many applications of wireless networks in defense and civilian fields. Military applications of MANET allow communications among soldiers and vehicles to form an information network, which is very sensitive to reliability and security.

One of the major challenges to deliver data in MANETs is selfishness [2]. Majority of the proposed protocols in MANET assume that mobile users are not selfish and they have the same degree of participation toward the other users. Selfish nodes want to maximize their individual benefits. For example, they may not relay messages of other nodes, or may willingly relay messages of their friends or the nodes inside their communities but not for strangers. A selfish node does not undergo with the packet transmission, it affects the performance of the network more solemnly. Some works are conducted for solving the selfishness problem. The main concern of these works is to detect selfish nodes, such as the work done in [3]. However, our concern is what to do after detection of the selfish nodes. In and, selfish nodes are isolated from route selection. This system depends on a centralized entity that monitors all the system parts to decide about nodes to isolate. Although isolation techniques outperform selfishness unaware techniques, they still suffer from the unbeneficial selfish nodes in the network and the overload they cause to its bandwidth. Moreover, the previous distributed techniques exchange a lot of information throughout the network, causing a huge overload on the network bandwidth and high consumption of the nodes power.

Therefore, it is highly desirable to suggest a mechanism which detects these kinds of misbehaving nodes in the network and provides an incentive to the selfish nodes to make them behave like other normal nodes.

II. LITERATURE REVIEW

Existing methods for detecting node misbehaviors can be classified into
(a) An Integrated Game Theoretical Approach
(b) Selfish Node Detection using Game Theory
(c) IDSM Based Approach using Individual Master Cluster Node
.

A. An Integrated Game Theoretical Approach

The problems of enforcing cooperation between nodes through an incentive scheme in MANETs have been received a great attention among researchers. Several secure routing protocols have been proposed to detect and mitigate the malicious and selfish node problems for MANETs, such as ARIADNE, CORE, SEAD and ASU. However, they could only take care of active attacks such Denial of Service (DOS), impersonation, black hole attack and wormhole attack. A fundamental issue need to be considered related to routing is how to perform efficient routing in dynamic network conditions of MANETs with the selfish nodes[8].

The incentive based mechanisms can be classified into three categories, namely reputation based mechanism, Virtual currency approach and Game theory model. The reputation based mechanisms isolate misbehaving nodes from cooperative nodes based on a reputation value received for cooperation of the node with its neighbors shown in Fig. 2.

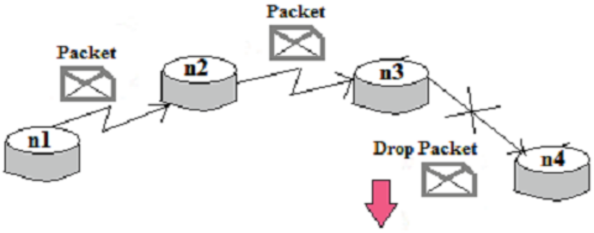


Fig. 2 Reputation based incentive mechanism

In the Virtual currency approach, cooperative node receives payments in the form of micro-currencies and earns their credits for forwarding packets to other nodes. The Game theory model is used to draw an optimal strategy for competitive players of the game and look for the Nash equilibrium state in which a player cannot raise his payoff by varying his playing strategies when other player strategies are remaining unchanged.[8]

A game theoretical approach is a mechanism for analyzing and modeling the nodes cooperation problem in MANET environment. Due to the dynamic network characteristics of MANTEs, such as unpredictable movements of nodes, dynamic topology conditions and lack of nodes cooperation, the process of monitoring and reporting the forwarding evidence history to the neighbor nodes is difficult to achieve in MANETs environment

Most of research works have been focused on various methods for detecting misbehavior nodes in the MANET environment. However, they have specifically focused on either incentive based approaches or game theoretical approaches to analyze the behavior of nodes in the network. In this work, misbehavior node detection and incentive based reputation scheme are integrated with the game theoretical approach called Supervisory Game to analyze the selfish behavior of nodes in the MANETs environment. The main advantage of integrating these approaches is to significantly reduce the misbehavior node detection cost in the network.

The Integrated Game Theoretical Approach

The I-GTA integrates malicious node detection process and incentive based reputation mechanisms with the game theoretical approach to minimize the malicious node detection cost. Malicious Node Detection Mechanism contains two phases namely 'Generation Phase' and 'Verification Phase'. The Generation Phase in turn includes routing task assignment confirmation phase, routing-report generation phase, and coordination-confirmation report generation phase. In the Verification Phase, a Supervising Agent (SA) verifies whether a node is legitimate one or a malicious node using the node detection algorithm.

In Supervisory Game Theoretical Approach the establishment of routes between a source node and a destination node is modeled as a supervisory game. The players are the nodes of the network. The network area is divided into logical regions called clusters. A cluster is a logical region of a network in which all nodes are well connected with each other by means of good quality bidirectional communication links.

In this work, an integrated supervisory game theoretical approach The selfish nodes gain their payoff when they relay packets for other nodes and reluctant nodes are punished and gradually isolated from the network. Nodes have to cooperate with others and relay packets for other nodes to maximize their bonus values. Due to the dynamic nature of MANET, the supervisory game theoretical approach is considered as a multi stage rating game that provides an optimal probability based incentive mechanism to maximize the payoff for cooperating players and ensure the timely delivery of packets to their destinations in MANETs.

B. Selfish Node Detection utilizing Game Theory

Game theory is a methodology used to analyze situations where two or more individuals or players, the outcome of an action by one of them not only depends on the action taken by that individual but also on actions taken by others. Players can be persons, company or any entity that can take decisions. In this context players are nodes in a network. It makes use of certain rules to strategically conclude successful and unsuccessful data transfer. A game consist of a case where two or more individuals, their choice of action has an impact on others.

Types of games in Game theory –

1. **Co-operative and Non – co-operative** – Co-operative games are those where players take decisions based on agreements with other players of the game. However, in non-co-operative games the players make moves to increase their own profit without any agreement with others.

2. **Normal Form Game and Extensive Form games** – Normal form games are those where utility of a player is represented in a matrix form, however in extensive games the utility is represented as a decision tree.

3. **Simultaneous Move games and Sequential games**

Simultaneous games are those where two players take a move at the same time. However sequential move games are those where players take move in some sort of defined sequence or order.

4. **Constant Sum and Zero Sum Games** – constant sum games are those where the result of all the possible strategies applied by players remains constant even if they are different. In zero sum games profit of one player is always a loss situation for another player.

5. **Symmetric and Asymmetric games** – in symmetric games the strategies adopted by players are similar. However, in Asymmetric games the strategies adopted by players are different.

Essentials of a Game

Players: these are the member that play game, they can be any individual, group or an organization or any entity that is capable of taking decisions.

Strategies: one or more choices or actions taken by the players while playing a game.

Outcome: this is a result of completion of one or more moves in a game. Pay-off: A reward or amount received for a given outcome.

Rules: these are those conditions that players have to follow while making a move in the game.

Dominant Strategy – a dominant strategy is a best move as compared to all other moves by all players in the game.

Nash Equilibrium – A combination of player’s strategies that are best response to each other. A game theoretic scheme to identify selfish nodes in the network and this is based on ESSDSR protocol which makes use of the battery resource for deciding the route between source and destination, where only node with high battery power will be selected to perform routing activity. Using a utility matrix we can show that nodes and network will only be benefited if they all work with co-operation between each other. So here we provide nodes with a reward to successfully perform routing of data. We provide nodes with a bonus point. Also since there is no acknowledgement sent in DSR protocols, we can verify by bonus point rewards we are giving the nodes after successful data transmission. After the successful data transmission the destination node will again send back another data packet back tracking the same path and allocating each node a bonus point , all those nodes that were a part of the data transmission activity.

A strategy is a plan of action through which a player must decide a valid possible move for the given situation. A strategy is said to be pure if at every stage in a game it specifies a move with complete certainty. A strategy is mixed if it applies some randomization to at least one of the moves.

For example in a game a player is person returning from work to home back, here his aim is to reach home as early as possible. He must make choices between selecting a bus, train and a subway. The first choice is to catch bus and second choice is to catch train and so on

- A person who always chooses to catch the train is a pure strategy

- A person who sometimes picks the train and sometimes bus is following a mixed strategy.

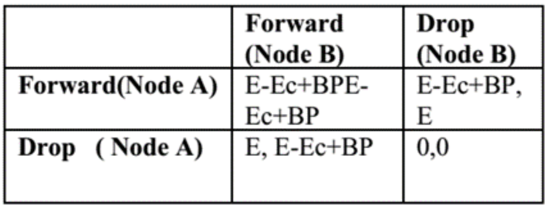
Games can be co-operative and non– Co-operative. Here we consider Non – Cooperative games. As described above a game has three components: players, set of actions, and a pay-off matrix shown in Table. 1 or utility function.

Assumptions for our game model –

- A network model consisting of n number of nodes are considered here
- Links in the network are symmetric and bi-directional
- Some nodes in the network may behave in a selfish manner to save their resources.
- Whenever any node forwards the data packet at that point of time it will have to lose its resources like battery power, else if the nodes are just dropping packets in that case no battery power is being consumed.
- Nodes have an identity and are given bonus points as a reward for successful transmission.

Variables used
Er = Remaining energy
E = Initial energy
Ec = energy consumed
BP= Bonus Point

Table 1: Pay-Off Matrix



	Forward (Node B)	**Drop (Node B)**
Forward(Node A)	E-Ec+BPE-Ec+BP	E-Ec+BP, E
Drop (Node A)	E, E-Ec+BP	0,0

In this game theory method it is show that a node to enhance the networks lifetime thereby identifying the selfish nodes in the network. Because selfish nodes will not forward any data to the nodes to save their resources. We have tried to modify the ESSDSR which is based on the battery consumption of the mobile nodes and finding out routes basis the high battery energy availability in the nodes. Also we have introduced the concept of rewards in the form of Bonus points assigned to the nodes that have helped in successful transmission of the data from source to destination. Nodes that do not have Bonus Point signifies they have never taken part in the data forwarding or routing activity. We can put them under suspect of selfish nodes, later on we can testify them by sending fake RREQ, if they reply they are normal nodes, else they are selfish nodes and hence we can isolate them for proper functioning of the network.

C. IDSM Based Approach using Individual Master Cluster Node

Selfish node Identification technique in MANET deals with the following issues which arise from constraints caused by their unique environments and applications are:

- Selfish node presence, network partitioning occurs more often in MANET.

- A major problem in MANET is network partitioning is when the server isolates the required data in a separate partition, thus occurs by reducing data accessibility to a large extent.
- Packet percentage received by the destination is equal to the number of packets sent by the source get affected by available number of selfish nodes in MANET.
- If Selfish nodes increases in MANET, Numerous intermediate hops in between source to destination get increased. It could lower the performance of the Network.
- Huge amount of packets dropped by the routers is due to the nodes acting as a selfish node for resource consumption.
- One Way delay is the time consumption which occurs due to the data packet be transferred across the MANET in between source node and the destination node. It increases by selfish nodes in MANET.

In this approach, it is presented that a IDSM approach using single master cluster-head is used. It monitors the nodes behavior for both inter-cluster and intra-cluster. In this proposed work, one head from each cluster is selected and then one master cluster-head is selected among different cluster-heads. This master head cluster node collects the information from the different cluster-heads, analyses the intrusion in the network. It then neglects the malicious nodes from the network. Further, it is used to increase the efficiency by decreasing the energy utilization in the network which results in the reliable service quality throughout the network.[9][11][14]

Selfish Node Behaviour

MAODV multicast as posturized in the Fig.3. In the below figure ‘S’ acts an source node, ‘M’ acts as an selfish node and ‘R1’, ‘R2’, ‘R3’ are the destined nodes which are presented as part of the network. The sender node ‘S’ in the first multicast group transfers the data packets to the receiver nodes inside the next multicast group. Here the node ‘M’ behaves as selfish, the packets routed on the S-RV1-RV2-M-R2 path are dropped by that node. Hence the receiver destined node ‘R2’ node does not received any packets, it only sends RREQs to its neighbors. Further if any RREPs not received, it sends THACK i.e., two hop acknowledgement for the reliable route detection and spots the selfish node as ‘M’ in the routing table. Another level of detection in selfish node are attained by the packet Transmission ratio and the every all node is compared with the cut-off ratio calculated distributively for each and every node.[15]

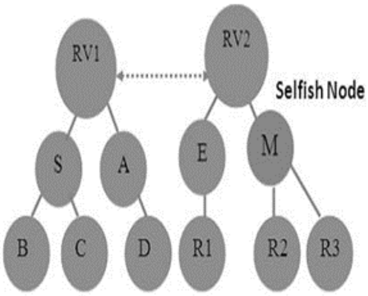


Fig 3. The Presence of Selfish Node in the Multicast Scenario of MAODV

MANET plays dominant part in the development of the information sharing, with the rapid advent in the wireless technology. MANET is easily prone to the intrusion because of two major reason; they are dynamic network topology and poor security measures. To overcome this issue, a framework is needed to provide a good information sharing system. This system creates an intrusion detection system; used to monitor the behavior of all nodes in the network along with that it detect and isolate the malicious node (or) nodes. A master cluster-head node gather data from the different cluster-heads, evaluate the presence of intrusion and later removes the malicious node from the network. Additionally, the efficiency is increased by the minimum energy consumption of the network and results in the reliable quality of service (QOS) throughout the network.[10][12][13]

III. CONCLUSION

A MANET has of a group of mobile device communicating through a wireless network. The MANET security has become most important. This survey paper discussed many methods to deal with selfish nodes. Selfish nodes are problem of ad hoc networks also they affect the network throughput. Among the above discussed strategies, in IDSM Based Approach the selfish node is detected and isolated, network efficiency is increased. It increases the efficiency by decreasing the energy utilization in the network which results in the reliable service quality throughout the network and evaluate the presence of intrusion and later removes the malicious node from the network.

REFERENCES

1. C. Siva Ram Murthy and B.S Manoj," Ad-Hoc Wireless Networks", Prentice Hall Communication engineering and Emerging Technologies Series, 2004
2. Wei Liu, Student Member, IEEE, Hiroki Nishiyama, Member, IEEE, Nirwan Ansari, Fellow, IEEE, Jie Yang, and Nei Kato, Senior Member, IEEE" Cluster-Based Certificate Revocation with Vindication Capability for Mobile Ad Hoc Networks" IEEE Transactions On Parallel And Distributed Systems, VOL. 24, NO. 2, FEBRUARY 2013.
3. Ningrinla Marchang, Member, IEEE, Raja Data, Senior Member, IEEE, and Sajal K. Das, Fellow, IEEE" A Novel Approach for Efficient Usage of Intrusion Detection System in Mobile Ad Hoc Networks" IEEE Transactions On Vehicular Technology, VOL. 66, Issue No. 02, May 2015.
4. C. K. Toh, Ad Hoc Mobile Wireless Networks: Protocols and Systems, Prentice Hall PTR, 2001
5. D. P. Agrawal and Q.-A. Zeng, "Chapter 13. Ad Hoc and Sensor Networks," Introduction to Wireless and Mobile Systems, Brooks/Cole-Thomson Learning, 2003, pp. 297–348.
6. Shih-Lin Wu ,Yu – Chee Tseng, "Wireless Ad-Hoc Networking : Personal Area , Local Area , and the Sensory Area Network",Auerbach Publications , 2007.
7. C. Vijayakumaran, T. Adiline Macriga," An Integrated Game Theoretical Approach to Detect Misbehaving Nodes in MANETs ", International Conference On Computing and Communications Technologies, 2017, pp. 180 - 173

8. Akansha Vij, Vishnu Sharma, Parma Nand, "Selfish Node Detection using Game Theory in MANET", International Conference on Advances in Computing, Communication Control and Networking, 2018 pp. 104 - 109
9. Neenavath Veeraiah, Dr.B.T.Krishna, "Selfish Node Detection IDSM Based Approach Using Individual Master Cluster Node", Second International Conference on Inventive Systems and Control, 2018, pp. 427 - 431
10. Dr.E.Mohan, Dr.A.Annamalai "Distributed Attack Detection For Wireless Sensor Networks " International Journal of Engineering & Technology, Volume 7 ,issue 6, 465-468 , 2018, (ISSN: 2227-524X).
11. Dr T.Suresh ,Dr K.T.Meena Abarna "Tracker Assisted Peer Scheduling Strategy in Multi-channel P2P VoD Streaming" International Journal of Computer Applications, Vol. 138, No 9,Mar 2016
12. R Anandha Lakshmi , Dr T. Suresh "A Relative Study of Various Routing Protocols in Mobile Ad Hoc Network" Asian Journal of Computer Science and Technology, Vol.7 No.S1, 2018, pp. 78-81ISSN: 2249-0701 ISSN:0975-8887
13. Gaurav Sharma, A.rajesh, L.Ganeshbabu and E.Mohan "Three-Dimensional Localization in Anisotropic Wireless Sensor Networks using Fuzzy Logic System" Ad Hoc & Sensor Wireless Networks, Volume45 , 29-57 , 2019
14. S. Arockia Babi Reebha, Dr T. Suresh and Dr K. T. Meena Abarna "An Efficient QoS Aware Clustering with Optimized firefly based Routing Protocol for Wireless Sensor Networks"ARCTIC Journal, Volume 73 Issue 3-2020, pp 148-182 ISSN: 0004-0843
15. Dr.E.Mohan, Dr.J.Sasikala et.al " Hybrid seagull and thermal exchange optimization algorithm- based NLOS nodes detection technique for enhancing reliability under data dissemination in VANETs " International Journal of communication systems, Volume 33 ,issue 14, 2020, *(*ISSN: 1099-1131)