International Journal of Future Generation Communication and Networking
Vol. 13, No. 4, (2020), pp. 3263–3277

An Efficient and Exhaustive Review on Selfish Node Detection Techniques for MANET's

1st Ramesh V , 2nd Dr.C.Suresh Kumar
[1]*Research Scholar, Department of Computer Science Bharathiar University*
Coimbatore, Tamilnadu - India
[2]*Principal , DR.Nagarathinam College of Engineering,* Namakkal, Tamilnadu - India

Abstract

In current days, mobile ad hoc networks (MANET) have developed into an emerging research area. MANET is an assortment of independent mobile nodes associated with one another with no focal facilitator. In MANET, utilizing the remote association, mobile nodes are associated and the nodes openly move where it needs to communicate with one another. One of the difficult issues in MANET is making sure about it in a unsafe environment. There is a few security issues emerge in MANET because of progressively changing network topology. At the point when a node attempts to endeavors the network holds for its own personal addition, yet reluctant to utilize its resources for different nodes in the MANET then these hubs are called selfish nodes. These sort of selfish nodes in the course corrupt the overall performance of the entire network. Be that as it may, in reality, most nodes may have a selfish behavior, being reluctant to forward packets for others so as to save resources. Consequently, distinguishing these nodes is basic for network performance. Numerous strategies are contrasting with improve the location of selfish nodes and improve the network performance and accuracy speed and network throughput and lessen the identification time of selfish node. In this paper we examined about the different selfish node detection strategies and propose a Modified Bates Distribution - Selfish Node Detection Technique (MBD-SNDT) for recognizing and disconnection of selfish node from the network.

Keywords— *mobile ad hoc networks, MANET, Modified Bates Distribution, MBD, Selfish Node Detection Technique, SNDT, Selfish node, Secure Incentive Protocol (SIP), Intrusion Detection System (IDS)*

I. INTRODUCTION

MANET represents Mobile Ad-Hoc Network additionally called as wireless ad hoc network or ad hoc wireless network that typically has a routable networking environment on top of a Link Layer ad hoc network. They comprise of set of mobile nodes associated remotely in a self-arranged, self-recuperating network without having a fixed framework. MANET nodes are allowed to move haphazardly as the network topology changes regularly. Every nodes acts as a routers as they forward traffic to other determined node in the network.

Because of significant progresses in mobile computing and remote correspondence innovation, cell phones have picked up sufficient correspondence, calculation, and memory assets to be interconnected. By means of definition, mobile ad hoc networks (MANETs) separate themselves from existing networks by the way that they depend on no fixed framework [1]. The network has no base stations, passages, distant workers, and so on All network capacities are performed by the nodes framing the network; every node plays out the usefulness of host and router, handing-off data to build up availability among source and destination nodes not straightforwardly inside one another's transmission range.

This component makes ad hoc networks financially practical since there is no cost associated with setting up or keeping up fixed network architecture. MANETs are independent, multi-hop networks interconnected through remote connections. The word ad hoc (deciphered with respect to this just from Latin) suggests that the network is shaped in an unconstrained way to fulfill a prompt need and specific

ISSN: 2233-7857 IJFGCN

objective. MANETs have a unique network topology. Since nodes in the networks are portable, with unhindered development, the configuration of the network topology can change quickly.

Ad Hoc Networks come up short on the framework seen in oversaw remote networks. Subsequently, nodes must assume the parts of router, server, and client, convincing them to collaborate for the right activity of the network [1]. Specific conventions have been proposed for specially appointed networks thinking about its impossible to miss qualities, yet in addition an ideal collaboration among nodes. By and large, it is expected that all nodes carry on as per the application and convention specifications. This presumption, notwithstanding, might be bogus, because of resource limitations (e.g., low battery power) or malignant behavior. Expecting an ideal conduct can prompt unanticipated entanglements, for example, low network efficiency, high resource utilization, and exposure to attacks. Thusly, a system that permits a node to gather the reliability of different nodes gets important.

Giving a trust metric to every node isn't just valuable when nodes act mischievously, yet in addition when nodes exchange data. As indicated by the worldview of autonomic networks [4], a node ought to be fit for self-configuring, self-overseeing, and self-learning by methods for gathering nearby data and exchanging data with its neighbors. In this way, it is significant to discuss just with dependable neighbors, since communication with getting into mischief nodes can bargain the self-sufficiency of ad hoc networks.

We surviving a flexible trust model dependent on the idea of human trust and apply this model to ad hoc networks. Our model forms, for every node, a trust relationship to all neighbors. The trust depends on past individual encounters of the node and on the suggestions of its neighbors. The proposals improve the trust assessment measure for nodes that don't prevail with regards to watching their neighbors because of resource imperatives or connection blackouts. The capacity of surveying the trust level of its neighbors brings a few favorable circumstances. Initial, a node can distinguish and detach noxious practices, trying not to transfer packets to malignant neighbors. Furthermore, participation is animated by choosing the neighbors with higher trust levels. Nodes learn dependent on the data exchanged with reliable neighbors to manufacture an information plane.

A mobile ad hoc network (MANET) [4] is moderately new correspondence worldview. The fast development of remote contraption, for example, laptop, PDAs remote sensors and Wireless telephones, shows the significance of remote innovation turning out to be more noticeable step by step. The infrastructure networks depend on a fixed base station or passage, where all the mobile nodes are associated with it. The infrastructure less networks is the ad hoc network, where all the mobile nodes are associated with one another with the nonappearance of a passageway a concentrated purpose of the board.

A mobile ad hoc network comprises of nodes. Nodes inside radio scope of one another can impart straightforwardly over remote connections, and those that are far separated utilize different nodes as transfers. Each node in a MANET additionally goes about as a router and routers are generally multi-hop. The dynamic and helpful nature of the ad hoc routing foundation likewise forces extra security dangers. Assaults against the ad hoc framework might be produced using outer or interior nodes. ad hoc routing algorithms depend on node collaboration, where every node may go about as a hand-off.

Dynamic variations to the network topology make it hard to recognize if a node giving bogus steering data is Byzantine or is simply out of sync with the topological changes. These extra security dangers must be thought of, when planning security systems for a wireless ad hoc network.

II. NETWORK INFRASTRUCTURE

There is no fixed or previous framework in an ad hoc network [1] all network functions (routing, security, network the executives, and so forth) are performed by the nodes themselves. Because of the nodes restricted transmission range, information spread is accomplished in a multi-hop design; nodes can thusly be considered as hosts and routers. In spite of the fact that the absence of framework opens another open door for assaults, the creators accept that the absence of infrastructure can assist with guaranteeing the survivability of the network in an antagonistic environment. This remains constant

ISSN: 2233-7857 IJFGCN

from a network security point of view, yet additionally when the clients of the network are under actual assault.

Ad hoc networks might be immediately framed with no from the earlier information on the actual area and network environment. MANETs' absence of framework in this manner makes it reasonable for different applications where traditional network miss the mark.

Hybrid ad hoc network join customary network foundation with multi-hopping. This subsidiary of ad hoc network will find useful application where fixed framework can be reached out through multi-hop networks or where the usefulness (and execution) of multi-hop networks can be upgraded by depending on some infrastructure.

III. LITERATURE REVIEW

Mobile Ad Hoc Network (MANET) is the collection of mobile nodes which form the network on the move without the need for any fixed infrastructure. It is a compilation of mobile nodes which converse with each other by means of a multi-hop wireless communication link. The nodes in the network act as host as well as router for the transmission of packets to distant nodes to establish communication. All the standard routing protocols for MANET are developed with an assumption that all the intermediate mobile nodes in the network are willing to forward the packets of other nodes. These are the services the network layer can offer. However, this protocol compliant behavior may not be achieved always due to the characteristics of the MANET. In some MANET‟s applications, all the nodes belong to a single authority and have a common goal to pursue (Merwe et al 2007) [1]. For example, emergency search and rescue, crowd control and law enforcement where all the nodes cooperate with each other. But in many civilian applications the nodes do not belongs a single authority and does not have a common goal.

In such networks, there is no guarantee that the nodes will forward the packets of other nodes by spending their limited resources like battery power and bandwidth. The nodes will try to preserve its resources by not forwarding the packets of other nodes but at the same time expects other nodes to forward its own packets to establish communication. This particular behavior is termed as selfish behavior. This misbehavior represents a potential danger to the communication in the network. Selfishness can be handled in two ways. One way is to punish the nodes i.e., to isolate the nodes, for being selfish in packet forwarding and another way is to reward the nodes which forward the packets of other nodes.

A secure trust model (Boukerche and Ren,2008) [2] that is developed with secure credentials, private keys, managing the trust value of nodes and decide the access rights to the node, this model is effectively identifying the malicious nodes in the system and exclude them from the network. Wang et al [3] has estimated a trust degree between the nodes they introduced a light weight trust based QoS model with the direct trust computation and neighbours node recommendation is observed, then they designed a trust base QoS routing algorithm (Wang et al) and provided results by comparing with AODV, watchdog-DSR and QAODV.

In this paper various research and techniques proposed to detect and isolate the selfish misbehavior has been addressed. Selfish behavior may lead to various security problems in the network such as throughput degradation, increase in end-to-end delay and packet loss which in-turn affects the overall performance of the network.

The authors (Tamilarasan & Aramudan 2011) [4] surveyed the challenges and proposals to mitigate performance degradation and network partitioning in MANETs. Most of the works to mitigate selfish behavior can be classified into Incentive-Based Mechanism, Reputation-Based Mechanism and other mechanisms. The incentive-based mechanism uses some incentive to motivate nodes to cooperate i.e., the node will get some incentives if it serves the network and pays back some price when it gains help from the network. Here the forwarding is considered as a service not a burden to the individual nodes. Reputation is the amount of trust inspired by a particular node in a specific setting or domain of interest. The nodes reputation can be obtained using direct observation or from reputation messages from other nodes in the network. Nodes that have a good reputation, because they helpfully contribute

ISSN: 2233-7857 IJFGCN

to the community life, can use the resources while nodes with a bad reputation, because they refused to cooperate, are gradually excluded from the community.

One of the most reputable works in this category is the nuglets has been proposed by (Buttyan & Hubaux 2001) [5]. In "Nuglets" the authors are concerned about the problem of non-cooperating nodes in civilian applications. These nodes tend to use the services provided by other nodes and is not ready to provide their services to other nodes. An economic approach is proposed to deal with the non-cooperating nodes in the mobile ad hoc networks. A charging mechanism called virtual currency (nuglets) is introduced for service usage. Nodes that use a service must pay for it to the nodes that provide the service. This mechanism encourages the nodes to make moderate use of the network.

Collaborative watchdog (Hernández-Orallo et al 2013) [6] approach and an analytical model that evaluates time of detecting the selfish nodes, they have extended the work incase selfish node increases a mean-max approximation for feasible computation.

A protocol on on-demand multi-path routing (Xia et al, 2013) [7] in mobile ad-hoc networks, the proposed system is feasible and flexible to find the shortest path to transmit the data packets in a secured method with malicious node detection. The proposed that in MANETs to reduce the hazards of the open connectivity in the network have presented a dynamic trust prediction model and evaluating the trustworthiness of the connected nodes and transmit the data packets and the result shown the effective in identifying malicious node.

RFSTrust model (Luo et al, 2009) [8] to evaluate the trustworthiness of node by fuzzy recommendation, thus it provide tolerance, packet forwarding review, the results show a great performance in fuzzy based recommendation.

The authors [Salehie and Tahvildari and Aliu et al.] [9] Define self-configuring as the capability to adapt autonomically and dynamically to environmental changes. Self-configuring has two main aspects as follows: i) installing, (re)configuring and integrating large, complex network intensive systems, and ii) adaptability in architecture or component level to re-configure the system for achieving the desired quality factors such as improving performance in response to environmental changes.

Wireless sensor networks connect deeply embedded sensors, actuators and processors. These networks are used for tasks such as surveillance, widespread environmental sampling, security and health monitoring. Sensor networks typically consist of hundreds to thousands of nodes that are generally stationary after deployment except for a few mobile nodes in the network. However, unlike cellular networks and mobile ad-hoc networks, these networks operate under severe energy constraints. While the operation of cellular networks is optimized for QoS, the operation of sensor networks has to be optimized to expend minimal energy in order to prolong the life of the network.

In packet trade model, the destination node pays for the service. The packet does not carry nuglets, but it is traded for nuglets by intermediate nodes. Each forwarding node buys the nuglets from the previous one for some nuglets and sells to the next forwarding node for some more nuglets. In this way, the forwarding node increases its number of nuglets by taking part in the forwarding service. The advantage of this model is that the source node does not need to estimate the total number of nuglets for the forwarding service.

The problem of stimulating cooperation in self-organizing mobile ad hoc networks for civilian applications is addressed by (Buttyan & Hubaux 2003) [5]. This approach uses the tamper resistant hardware module called security module in each node. This security module maintains a nuglet counter and this counter is incremented by one when the node forwards a packet and it is decremented by one when it sends its own packet. The value of the nuglet counter should be positive in order to send its own packets. This approach ensures that the selfish nodes does not earn enough nuglets in order to send its own packets thereby stimulating the selfish nodes to take part in packet forwarding to earn the sufficient nuglets to send its own packets.

The authors (Zhong et al 2003) [10] have proposed an incentive for mobile nodes to cooperate and report actions honestly and it does not require any tamper-proof hardware at any node. When a node receives a message, the node keeps a receipt of the message. Later, when the node has a fast connection

ISSN: 2233-7857 IJFGCN

to a Credit Clearance System (CCS), it reports the CCS the messages that it has received / forwarded by uploading its receipt. The CCS then determines the charge and credit to each node involved in the transmission of a message depending on the reported receipts of a message. This is the first pure-software solution that has formal proofs of security. First the system provides incentive to selfish nodes to cooperate and then it determines charge and credit from a game-theoretic perspective and motivates the nodes to report its actions honestly.

A credit-based protocol to stimulate cooperation among mobile nodes in packet forwarding in order to improve the network performance by mitigating the selfish behavior have proposed by (Zhang et al 2007) [11]. Secure Incentive Protocol (SIP) is implemented in the secure module of each node. During session initialization, the source negotiates session traffic information with the destination and intermediate nodes along the route path and various session keys for securing SIP operations are established during the session–key establishment phase. During the rewarding phase, each intermediate node is awarded a certain number of credits commensurate with the service they provided to the source and the destination.

The authors (Mahmoud & Shen 2012) [12] proposed a fair, efficient and secure cooperation incentive mechanism for multi-hop wireless networks to thwart selfishness attacks and to stimulate node cooperation in order to improve the network performance and fairness. The fairness is achieved by charging both the source and destination nodes of the communication.

A third party Accounting Centre (AC) is used to store and manage the credit accounts of the nodes, and generate private/public key pair and certificate with unique identity for each node. Instead of generating a check per message, a small- size checks containing the payment data for all the intermediate node is generated per route. The nodes can contact the accounting centre at least once every few days and this connection can occur via the base stations or the wired networks such as internet.

The FESCIM has been proposed to work in two modes namely hybrid mode and pure ad hoc mode. In hybrid mode, at least one base station is involved in communication. The source node transmits its messages to the source base station, if necessary in multiple hops. If the destination resides in a different cell, the messages are forwarded to the destination base station that transmits the messages to the destination node possibly in multiple hops. In pure ad hoc mode, the messages are sent and received without involving the base station. This method was implemented using DSR protocol and the performance was compared with Sprite and Express.

The authors have introduced two extensions to the Dynamic Source Routing (DSR) (Johnson & Maltz 2004) [13] to mitigate the effects of routing misbehavior: The watchdog and the pathrater. The watchdog identifies misbehaving nodes by listening in the promiscuous mode, while the pathrater avoids routing packets through these nodes. Dynamic Source Routing (DSR) protocol is another reactive routing scheme with a difference that packets carry route information from source to destination. Packets may not rely upon hop-by-hop forwarding instead source learnt routes are inserted into packets. RREQ and RREP are used in DSR similar to that of AODV. RREQ is broadcast by source nodes through neighbors and propagated to further after neighbors have updated their routes to source and adds their own address to the accumulated path in the RREQ and propagate the RREQ through its neighbors until destination is reached. Each of the intermediate nodes may update their routes to any node in the accumulated in the received RREQ. If node is destination, RREP is prepared with accumulated route from source to destination in RREQ and unicasted upstream. To search multiple routes to destination node, DSR uses route cache which contains information about multiple routes to the same destination. RERR is initiated when link break is noticed by upstream nodes towards source.

CORE (Michiardi & Molva 2002) [14] is a generic mechanism based on reputation to enforce cooperation among the nodes of a MANET to prevent selfish behavior. Each network entity keeps track of other entities collaboration using a technique called reputation. The reputation is calculated based on various types of information on entitys rate of collaboration. The CORE scheme consists of the following three components: network entity, reputation table and the watchdog mechanism. The network entity is nothing but a mobile node and each node is having a set of Reputation Table (RT)

ISSN: 2233-7857 IJFGCN

and a Watchdog Mechanism (WD). The CORE scheme uses two types of protocol entities, a requestor and one or more providers.

CONFIDANT protocol (Buchegger & Boudec 2002) [15] is developed to make misbehavior unattractive. CONFIDANT consists of the following components: the monitor, the reputation system, the path manager and the trust manager. The monitor registers the deviation from the normal behavior and calls the reputation system as soon as a given bad behavior occurs. The reputation is built on negative experience rather than positive impressions. The path manager re-rank the paths according to security metric, deletes the path containing malicious nodes and takes action on receiving a request for a route from a malicious node. The trust manager deals with incoming and outgoing ALARM messages. ALARM messages are sent by the trust manager of a node to warn others of malicious nodes. Outgoing ALARMs are generated by the node itself after having experienced, observed a report of malicious behavior.

A reputation-based system has been proposed (Liu & Yang 2017) [16] to locally update the reputation of mobile nodes. Given an initial assessment of the reputation of other mobile nodes, the system shows that under mild conditions, the mobile nodes will achieve reputation agreement. The analysis captures reputation propagation using graph connectivity. The convergence speed of two reputation propagation mechanisms is evaluated through simulations and the results show that the speed of reputation propagation is an important factor for the convergence speed of reputation agreement.

In Friends and Foes (Miranda & Rodrigues 2003) [17], the author proposes a novel algorithm that aims to discourage selfish behavior in mobile ad hoc networks. It presents a long lived memory that allows nodes to be rewarded by services provided in the past but also does not charge by the number of hops used. This supports the management of fairness by allowing nodes to publicly declare that they refuse to forward messages to some nodes. Every node maintains the following variables: friends, foes and selfish.

The objective of OCEAN (Observation-based Cooperation Enforcement in Ad hoc Networks) is to use first-hand observations of other nodes behavior to detect and mitigate misleading behavior in ad hoc networks. OCEAN (Bansal & Baker 2003) [18] outperforms the schemes requiring secondhand reputation exchanges in terms of network throughput. The work addresses the attacks at the routing layer and do not attempt to address attacks at lower layers or passive attacks like eaves dropping and also do not deal with issues like node authentication, securing routes. OCEAN encourages the proper routing participation. It considers two types of routing misbehavior namely misleading and selfish behavior.

The authors (He et al 2004) [19] proposed a Secure and Objective Reputation-based Incentive (SORI) framework for mobile ad hoc networks where packet forwarding is encouraged and selfish behavior is punished. The unique features of SORI scheme are that the reputation of a node is quantified by objective measures, the propagation of reputation is secured by one-wayhash chain based authentication scheme and the reputation of a node is only propagated to neighbors which reduces the communication overhead

A reputation-based mechanism to detect and isolate the selfish nodes has been proposed by (Refaei et al 2005) [20]. The reputation of a node is assessed automatically based on the completion of the required service(s). This reputation evaluation scheme is implemented individually at every node in the mobile ad hoc network. Each node maintains a lookup table and reputation table. The lookup table maintains information regarding the data packets forwarding through it and the reputation table maintains the reputation index of the nodes immediate neighbors. The reputation index is increased for each successful transmission and it is decreased for failed transmissions. of the number hops between the source and the failed node. Often single feature routing protocols suffers from limitation due to its very mode of operations. Combining the best of two or more classes of protocols often covers the limitation of other class. Hybrid routing protocols combines the features of both reactive and proactive routing protocols and attempt to overcome the limitations of each class of protocols through some customizations in basic operation modes of constituting members. ZRP (Zone Routing Protocol),

ISSN: 2233-7857 IJFGCN

SHARP (Sharp Hybrid Adaptive Routing Protocol, DHAR (Dual-Hybrid Adaptive Routing) & ADV (Adaptive Distance Vector Routing), TORA etc. are the representative proposal in this categories.

Self-policing mechanism (Buchegger & Boudee 2005) [21] based on reputation to enable mobile ad hoc networks to keep functioning despite the presence of misbehaving nodes is described. Node misbehavior can be detected with the help of local observation and the use of second hand information from neighboring nodes. Upon detection, the misbehaving node is isolated from the network.

A global reputation-based scheme (Rekha & Jyoti 2011) [22] for the detection and isolation of selfish nodes has been addressed. A cluster head is used for reputation management of each node in the network. Detection of selfish nodes is accomplished which are created due to nodes conserving their energy using NS2. After their detection, performance analysis of network with selfish node and the network after isolation of selfish node is carried out. The results reveal that the network throughput and packet delivery fraction increases with the proposed approach.

Audit-based Misbehavior Detection (Zhang et al 2016) [23] designed in wireless networks to address the issue of recognizing and separating misbehaving nodes that decline to forward packets in multi-hop ad hoc networks. A system called Audit-based Misbehavior Detection (AMD) is designed effectively and efficiently separates both continuous and selective packet droppers. The AMD system incorporates reputation management, trustworthy route discovery, and identification of misbehaving nodes based on behavioral audits.

An add-on technique for routing schemes to detect misbehaving links and to mitigate their adverse effect called 2ACK is proposed by (Liu et al 2007) [24]. This scheme sends two-hop acknowledgement packets in the opposite direction of the routing path only for a fraction of the received packets which reduces the additional routing overhead. Suppose that N1, N2 and N3 are three consecutive nodes along a route. The route from a source node, S, to a destination node, D, is generated in the route discovery phase of the DSR protocol. When N1 sends a data packet to N2 and N2 forwards it to N3, it is unclear to N1whether N3 receives the data packet successfully or not. Such an ambiguity exists even when there are no misbehaving nodes.

The combinations of reputation and incentive-based mechanism have proposed (Al-Karaki & Kamal 2008) [25]. The virtual currency schemes provide more fairness than the reputation-based schemes. However, the cooperation between nodes in reputation-based schemes is better. This model combines the features of virtual currency and reputation-based schemes. This mechanism is protected from abuse by its fully distributed nature and hence there is no need to implement it in a tamper resistant hardware module. This mechanism protects the networks from the abuse.

A new solution is proposed to monitor, detect and safely isolate misbehaving nodes (Djamel & Nadjib 2009) [26] that do not forward a packet that aims at improving the efficiency in detecting and isolating misbehaving nodes with a minimum overhead. The solution is structured around five modules: the monitor, the detector, the isolator, the witness, and the investigator. The monitor module is responsible for controlling the forwarding packets. For the monitoring, the authors proposed the efficient technique of random two-hop ACK, which reduces the cost. The detector module, which is in-charge of detecting the misbehaving of monitored nodes, uses Bayesian approach enabling redemption before judgment. The isolator, responsible for isolating misbehaving nodes detected by the detector uses the witness-based protocol, for both data and control packets to isolate a detected node, to be executed cooperatively by the isolator, the witness and the investigator. The investigator module is investigates accusation before testifying when the node has not enough experience with the accused. The witness module is responsible of providing testimonies against suspicious nodes.

Anomaly detection scheme in MANET is based on a dynamic learning process as illustrated by (Nakayama et al 2009) [27] which permit the training data to be updated at the particular time intervals. The dynamic learning process engages the projection distances based on multidimensional statistics and a forgetting curve. Dynamic Anomaly Detection (DAD) scheme is classically used to substantiate the uniqueness and the topology of the network but the study is not feasible on analyzing the more intelligent isolation schemes.

ISSN: 2233-7857 IJFGCN

Context-free (COFFEE) protocol (Chengqi & Qian 2010) [28] proposed for stimulating packet forwarding which can transmit packets through the route path without knowing whether the intermediate nodes are selfish or not. The context means recorded information on nodes behavior, goodness or selfishness, and so on. The packets are transmitted from the source by hiding the identity of the destination from all nodes on the path. The destination node also acts as an intermediate node in the forwarding process. The identity of the destination is revealed after all nodes complete its forwarding process successfully.

The authors (Wu & Yu 2010) [29] presented a threshold-based technique to detect the selfish node and to decrease the false detection rate. These misbehaviors of the selfish nodes reduce the efficiency, the reliability and the fairness in MANET. Though the selfish nodes do not harm the network, the number of selfish nodes increases, they will cause the degradation of the network performance.

Barani (2014) [30] has proposed the hybrid approach for detection of dynamic intrusion in Ad Hoc Networks. The working of this proposed approach is based on the combination of Genetic Algorithm (GA) and Artificial Immune System (AIS) given by GAAIS, for detecting the dynamic intrusion in AODV-based MANETs. GAAIS has the ability to adapt itself based on the changes in the network topology by means of two updating methods such as partial and total.

Each normal feature vector obtained from the network traffic has been represented by means of hyper sphere having fix radius. The non-self-space has been covered by using Niche MGA algorithm and the set of spherical detectors have also been generated. The generated spherical detectors are useful for detecting any anomaly present in network traffic. The performance evaluation of this scheme has been done based on several experiments conducted for detection of specific routing attacks namely flooding, black hole, neighbor, rushing and wormhole.

Intrusion Detection System (IDS) is proposed by (Debdutta Barman & Rituparna Chaki 2011) [31] based on mobile agents. The mobile agents travel through the network gathering vital information which can be processed by the agents later. It reduces the network bandwidth consumption by moving thedata analysis to the location of intrusion. Information processed by mobile agent helps to detect the attacker. The destination node does not respond correctly to the source node.

The N-ACK Scheme (Usha & Radha 2011) [32] to isolate the misbehaving nodes in MANET requires an end-to-end ACK packet to be sent between source and destination. The destination on receipt of data packets sent by source must respond with NACK packet. Each node maintains a list of data packets sent and forwarded. As soon as a node initiates a data packet as a source, it adds the id of the packet to the list of data packet sent. As the node receives the NACK packet for the data packet it removes the corresponding data packet id from the data packet sent list. It provides a better way to counter most of the misbehaving nodes in MANET without compromising the throughput of the network.

Fighting against packet dropping misbehavior (Baadache & Belmehdi 2012) [33] presented in multi-hop wireless ad hoc networks. The approach is used to verify the correct forwarding of packets by an intermediate node. In multi-hop wireless ad hoc networks, the packets are forwarded through intermediate nodes beside the source–destination path. Lacking the control on packet forwarding, an intermediate node perform selfishly or maliciously to reduce the packets going through it. The dropper motivation is the conservation of its resources with limited energy or the initiating the rejection of service attack. A technique is designed to authenticate the correct forwarding of packets using intermediate node.

In MANET, each and every node has to cooperate in routing and data forwarding tasks because cooperation reduces the consumption of battery power. Resource constraints of MANET node obtain dynamic selfish behavior i.e. not cooperating with routing operation and hence it lead to dreadful condition of the network performance. For this case, (Hussain et al 2012) [34] explained a proactive mechanism. Initially, simulation based study is carried out to estimate the effects of selfish nodes on network performance. After that on the contrary with selfish node, detection approaches are based on fully watchdog methods by means of promiscuous monitoring. A proactive mechanism is designed to

ISSN: 2233-7857 IJFGCN

identify the nodes that are displaying selfish behavior based on the factors which derives selfish behavior and mitigate its effect on network performance.

[Hernandez-Orallo et al., 2015] [35] has described the novel method to detect the selfish nodes called as collaborative Contact-Based Watchdog (CoCoWa) mechanism. This new CoCoWa scheme has combined the local watchdog detection approach followed by the gathered data dissemination in the MANET to detect the selfish nodes. In case of one node detecting a selfish node, the information gathered by it previously can be transmitted to other nodes during the contact. By this method, the nodes can receive warning information with regard to selfish nodes in the MANETs. This method has aimed in reducing the detection time and he effect of both false negatives and false positives for overall improvement of the precision. The experimental result has also shown that the overall detection time has been reduced by the CoCoWa approach without using any collaborations scheme.

A collaborative contact based watchdog mechanism (Hernández- Orallo et al 2012) [35] supported with the contact distribution of the identified selfish nodes based on fast diffusion of selfish nodes awareness is developed. Analytical model used to evaluate the time of detection and number of message of collaborative watchdog approach. With this collaborative approach, a systematic representation is presented to estimate the discovery time essential to recognize the misbehavior nodes. Location augmented routing also include geographical information besides proactive or reactive routing techniques. To know geographical information global positioning system (GPS) helps in obtaining actual geographic coordinates on some stable coordinate system is used. Control packets and data packets are sent in general direction of the destination if recent geographical coordinated for that destination are known. Thus geo location information can help to stop destination search in the whole network. It is helpful in reducing control overheat in network provided all nodes must able to access their geographical information continuously. Network can rely on location based routing to accomplish scalability.

Misbehavior is one of the common problems in MANET as it may cause severe damage to the whole network. The authors (Aishwarya et al 2013) [36] proposed an acknowledgement-based approach named I-2ACK for the detection and isolation of misbehaving nodes from the network. I-2ACK is based on sending acknowledgement packets for reception of data packets and using simple rating mechanism for counting the number of data packet such that it overcomes the problem of misbehaving nodes. The performance of I- 2ACK has been compared with other acknowledgement-based schemes and the results shows that the I-2ACK performed better in the presence of misbehaving nodes.

Liu et al. (2007) [11] has employed a cache scheme by which the selfish nodes have been detected in MANETs. This scheme has enabled the detection of the misleading nature of the selfish nodes by means of the proposed hardware. The mobile nodes which optimize its own benefits but ignore the benefit of neighboring nodes are usually termed as selfish nodes. By means of this cache system, the selfish node can be detected for the mechanism for dropping all the packets or only the data packets. After identifying misbehaving nature of the node, the report is usually sent by the hardware to other neighboring nodes. This data report was found very helpful for other nodes in protecting the entire network from misbehavior. In this scheme, a single node could ensure the difference s between software and hardware. Despite the misbehaving nature of the software, the employed hardware has resistance towards the damage and hence considered as the key feature for bringing the trust relationship among mobile nodes of MANETs.

It proves that a self-deploying network greatly reduces the number of base stations required as compared to a statically deployed network. It explores the concept of robotic, wireless base stations and discusses their behavior subject to principles inspired by Asimov's Law of Robotics. This paper introduces the concept of robotic base stations which would automatically sense their environment based on different types of measurements and use these to adapt various parameters and possibly even their position. The backhaul for the robotic base stations would be provided via wireless links to an anchor point acting as a gateway to an IP network.

In order to determine, the target cell for handover (Lobinger et al.) [37], each cell first prepares a list of candidate cells that could be possible targets. It then estimates the load condition of these cells and

ISSN: 2233-7857 IJFGCN

the impact of changing the handover parameters on the load of the cell. Load estimation is done based on SINR prediction and utilizes UE measurements. The authors prove through simulation that the average number of satisfied users can be improved with the load-balancing algorithm and the proposed metric for load estimation.

Simulation results of a self-optimizing LTE network (Lobinger et al.) [37] which uses two algorithms change different parameters but control the same decisions related to handover. Through simulations, the authors demonstrate the interaction between the two algorithms, which each capable of reducing the impact of the other. One proposed solution to avoid this is to combine the two algorithms into a single function, thus eliminating the need for them to explicitly interact and co-ordinate with each other. However, this cannot be done for all SON functions and the need is for a more generic approach to handle interactions between different SON algorithms.

The authors propose one such approach of introducing a SON function which looks at the KPI metrics and uses these to control the two algorithms by limiting their optimization actions. The algorithms adapt their control parameters based on the KPI metrics if necessary. Simulation results show system performance comparable to the individual performance of the two algorithms and in some cases better than that of the individual algorithms. The advantage of this solution is that the individual SON algorithms stay unchanged and a new module called the coordinator takes control on top of them.

(Kant and Chen) [38], discuss the disadvantages of APS based mechanisms for wireless networks. In addition to being expensive, the APS mechanisms do not take the priority of the applications into account. Since, each application has its own service survivability requirements; this approach of switching all application en masse is unacceptable. This work proposes a multi-layer mechanism to provide service restoration. They propose the use of SCTP as the transport protocol instead of TCP. SCTP is preferred because of its support for multi-homing. The fault management module of the system determines the active interfaces and constantly monitors their load. In the event of an interface failure or congestion on a link associated with an interface, the affected applications are switched to an alternate interface.

Mobile Agent Based Detection for Selfish Node (MADSN) (Roy & Chaki, 2011) [39] detection in which the necessary information has been gathered by the mobile agents when it travels through the network. The gathered vital information can then be processed by the mobile agent itself. The selection of threshold value was considered as a key step as it had offered the way to detect the attacker far earlier as possible.

Moreover, the consumption of network bandwidth has been considerably reduced network bandwidth owing to the movement of the data computation towards the place of the intrusion. This unique mobility feature of MADSN has resulted in increased efficiency of each node thus causing subsequent increase in overall performance of the network.

Liang et al. proposes a Secure and Reliable Routing framework for Wireless Body Area Networks (WBANs) [40]. Wireless Body Area Networks consist of a network of sensors to monitor bodily functions. The data from these sensors is then aggregated and sent over the Internet to a central monitoring entity. Although these networks are small in size and extremely localized, bodily movements subject them to frequently changing topologies and correspondingly the routing algorithms must adjust to this quickly to allow reliable data transfer of critical data. The authors propose a framework in which each node measures the link quality of all its neighbors. Using past link quality measurements, the nodes predict the incidental quality of a link. When the routing algorithm has to select among a set of candidate nodes, it uses the one with the best link quality.

Each node uses an auto-regression model to predict the link quality. Auto-regression models are used for modeling of time-series data and to predict the value at a particular instant of time. When a node sends a data packet, all nodes listen to the transmission, even though it is not destined to them. These nodes respond back with an ACK to the sender node, the ACK packet containing the received signal strength. The sender node uses this to update the link-quality measurement that it maintains. A node which does not respond with an ACK is marked as unreachable by the sender node. Through simulations, the authors prove that the proposed technique improves the routing reliability because one

ISSN: 2233-7857 IJFGCN

of the best links is chosen for transmission at each point, and the probability of sending a packet to a dead or a non-existent node is minimal.

IV. MODIFIED SKELLAM DISTRIBUTION -BASED SELFISH NODE DETECTION TECHNIQUE (MSD-SNDT)

The projected Modified Bates Distribution - Selfish Node Detection Technique (MBD-SNDT), the detection and separation of selfish nodes include

1. Intention of mean packet deviation,
2. Assessment of variance and standard deviation for computing MBD and
3. Detection and separation of selfish node.

Mean Packet Drop

If the quantity of packets forwarded and obtained by using every node 'i' is PF(1) , PF(2) ,…....., PF(s) and PR(1) , PR(2) ,....., PR(s) respectively as monitored by every of its buddies in's' sessions. The range of packets dropped via every mobile node as monitored via their neighbors in every consultation 'k' is

$$DROP_{PACKET(k)} = PR_{(k)} - PF_{(k)} \quad (1)$$

The mean packet drop is

$$MDROP_{PACKET(k)} = \sum_{k=1}^{s} \frac{DROP_{PACKET(k)}}{S} \quad (2)$$

Total variance

The total variance is

$$T - VAR_{DETECT} = \sum_{c=1}^{s} \frac{(PR_{(C)} - MDROP_{PACKET(C)})}{S} \quad (3)$$

The MBD computed based on (3) and (4) is

$$(BDITF)_{DETECT} = \frac{S}{S-1}\left(1 - \frac{\sum_{k=1}^{s} DROP_{PACKET(k)} * PR_{(k)}}{T - VAR_{DETECT}}\right) \quad (4)$$

The mobile nodes recognized by way of MBD less than 0. 35 (received from simulation) are detected as selfish node misbehavior.

Proposed Algorithm

The subsequent algorithm illustrates the stairs involved in detecting selfish node misbehavior the use of MBD and keeping apart them from the multicasting activity.

1. Let N be number of nodes.
2. GN – Group of nodes of the routing path, SN (the source node) and DN (the destination node) respectively.
3. The cell node which is prepared for statistics transmission acknowledges SN through `RREP' message.
4. Allow this set of rules step (5 -12) be accomplished for a node 'n' wide variety of sessions for transmission.
5. For every node 'u' of GN in the routing course
6. Estimate
   $DROP_{PACKET(k)} = PR_{(k)} - PF_{(k)}$
7. Compute
   $MDROP_{PACKET(k)} = \sum_{k=1}^{s} \frac{DROP_{PACKET(k)}}{S}$

ISSN: 2233-7857 IJFGCN

8. Calculate

$$T-VAR_{DETECT}=\sum_{c=1}^{s}\frac{(PR_{(C)}-MDROP_{PACKET(C)})}{S}$$

9. Estimate

$$(BDITF)_{DETECT}=\frac{S}{S-1}\left(1-\frac{\sum_{k=1}^{s}DROP_{PACKET(k)}*PR_{(k)}}{T-VAR_{DETECT}}\right)$$

10. If (MBD(u) < 0. 35) then
11. Node u is selfish node misbehavior compromised
12. Name selfish_node_attack-mitigation (u)
13. Else
14. Node u is reliable
15. End if
16. End for
17. End

V. SELFISH NODES

Consolidate exertion of nodes in mobile ad hoc network [41] makes it all the more remarkable. Be that as it may, supporting a MANET is a cost-escalated movement for a mobile node. Route discovery and packets forwarding devours data transfer capacity and energy. One such routing misbehavior of node is a few nodes might be go about as selfish by participating in route discovery and upkeep measure, however deny sending the packet. Such sort of misbehavior, reduces packet delivery conveyance proportion and furthermore debase framework execution as far as force and transmission capacity. MANETs is needed brought together observing and infrastructure-less conduct makes it more helpless against assault, and hard to distinguish selfish node adequately.

The data spread among the remote nodes in an ad hoc environment [42] mostly relies upon the participation kept up between them. This co-activity is fundamental for building up both forward and turn around route just as handing-off the packets. Because of the restricted accessibility of resources in an ad hoc situation, a portion of the nodes may will in general drop the packets originating from their neighbor nodes while sending their own packets. This sort of node's behavior is known as "Selfish Behavior".

All nodes present inside the network are liable for sending packets to its neighboring nodes [43]. Numerous resource requirements like CPU power, battery, data transmission and a portion of the nodes may pass on packet sending towards its resource decrease. The selfish node conduct presence prompts leads the network and has a negative effect in the activity of the network. To defeat such conditions selfish node finding is required.

There is a few security issues emerge in MANET because of progressively changing network topology [44]. The dependable communication is accomplished just when there exists collaboration among the mobile nodes in MANET. Because of the absence of resources some mobile nodes will not advance the forward packet to different nodes. This sort of nodes is known as the selfish nodes.

In the DTN (DELAY TOLERANT NETWORKS) [45] there is not at all base station as present in existing wireless networks. To convey a message DTN utilizes store, convey and forward Policy. There are various nodes present in the environment as some of them are pernicious nodes. A selfish node is a node which drops all messages which are gotten to spare its own personal energy..

VI. CONCLUSIONS

At last, the extended Modified Bates Distribution - Selfish Node Detection Technique (MBD-SNDT) that can identify the selfish nodes successfully by considering the forward and contact history proof with lesser time utilization is introduced. The presentation of this framework is estimated by a few exhibition measurements and it is presumed that the proposed framework works in a way that is

ISSN: 2233-7857 IJFGCN

better than the current frameworks. The time taken for recognizing selfish nodes is impressively low, when contrasted with the overall strategies.

The proposed framework shows a decent level of data availability, which implies that the data can be gotten to productively, with no bottlenecks. The data is available with no issues, in light of the fact that the regularly gotten to data items are dispensed appropriately. This proposed MBD-SNDT became given the utilization of variance and mean packet forwarding rate for assessing the level of effect achieved through the selfish qualities of mobile node toward the network with the end goal that right location and segregation of selfish nodes can be forced for strengthening the level of network overall performance.

REFERENCES

[1] vander Merwe, J., Dawoud, D., and McDonald, S. 2007. A survey on peer-to-peer key management for mobile ad hoc networks. ACM Comput. Surv. 39, 1, Article 1 (April 2007), 45 pages DOI 10.1145/1216370. 1216371

http://doi.acm.org/10.1145/1216370.1216371.

[2] Ren, Y. and Boukerche, A. (2008) Modeling and Managing the Trust for Wireless and Mobile Ad Hoc Networks. IEEE International Conference on Communications, 2008. ICC'08, Beijing, 19-23 May 2008, 2129-2133. http://dx.doi.org/10.1109/icc.2008.408.

[3] Wang, W., Huang, K., &Zou, Y. (2016). Cooperation incentive mechanism for selfish users based on trust degree. 2016 Sixth International Conference on Information Science and Technology (ICIST), 2(1), 12-25.

[4] Tamilarasan S, Aramudan, "A Performance and Analysis of Misbehaving node in MANET using Intrusion Detection System" IJCSNS International Journal of Computer Science and Network Security, VOL.11 No.5, May 2011 pp. 258-264.

[5] Levente Buttyán & Jean-Pierre Hubaux, "Stimulating Cooperation in Self-Organizing Mobile Ad Hoc Networks" , Springer - Mobile Networks and Applications , Vol. 8, pp. 579–592(2003).

[6] Hernández-Orallo, E., Olmos, M. D., Cano, J., Calafate, C. T., & Manzoni, P. (2013). A Fast Model for Evaluating the Detection of Selfish Nodes Using a Collaborative Approach in MANETs. Wireless Personal Communications, 74(3), 1099-1116

[7] Hui Xia, Zhiping Jia, Xin Li, Lei Ju, Edwin Sha, "Trust Prediction and Trust-based Source Routing in Mobile Ad Hoc Networks" , Elsevier - Ad Hoc Networks , Vol.11 Issue.7 , pp.2096-2114 , 2013

[8] Junhai Luo , Xue Liu, Mingyu Fan , "A trust model based on fuzzy recommendation for mobile ad-hoc networks" , Elesvier - Computer Networks , Vol. 53 pp. 2396–2407, 2009

[9] Mazeiar Salehie, Ladan Tahvildari, "Self-adaptive software: Landscape and research challenges" , ACM transactions on autonomous and adaptive systems (TAAS), Vol.4, Issue 2, pp. 1-42, 2009

[10] Cheun Ngen Chong, Zhonghong Peng, and Pieter H. Hartel, "Secure Audit Logging with Tamper-Resistant Hardware" , Springer - IFIP — The International Federation for Information Processing Book Series – Vol. 122, pp 73-84 , 2003

[11] Yanchao Zhang, Wenjing Lou, Wei Liu, Yuguang Fang , "A secure incentive protocol for mobile ad hoc networks" , Elesvier - Wireless Networks , Vol.13 Issue 5 , pp- 569-582, 2007

[12] Mohamed M. E. A. Mahmoud, Xuemin (Sherman) Shen, "Security for Multi-hop Wireless Networks", book series : Springer Briefs in Computer Science, pp 1-9 , 2014

[13] Johnson D, Dynamic Source Routing for Mobile Ad Hoc Networks, IEFT MANET Draft, April 2003

[14] Pietro Michiardi and Refik Molva, "Core: A Collaborative Reputation Mechanism to Enforce Node Cooperation in Mobile Ad Hoc Networks" Book Series – Springer - IFIP — The International Federation for Information Processing, IFIPAICT, volume 100 , pp 107-121

[15] Sonja Buchegger, Jean Yves Le Boudec , "Performance analysis of the CONFIDANT protocol" , ACM - MobiHoc '02: Proceedings of the 3rd ACM international symposium on Mobile ad hoc networking & computing, pp. 226–236, June 2002 https://doi.org/10.1145/513800.513828

ISSN: 2233-7857 IJFGCN

[16] Yang Yang , Xiaoyu Jin, Su Yao, Xuesong Qiu, Liu Liu , "Reputation detection based on incomplete β distribution for mobile agent in wireless sensor networks", International Journal of Distributed Sensor Network , Vol. 13 issue 6, pp. 1-13 2017

[17] Miranda H and Rodrigues L , "IEEE International Workshop on Mobile Distributed Computing (MDC)" , pp. 1 -13, 2003.

[18] Sorav Bansal, Mary Baker, "Observation-based Cooperation Enforcement in Ad Hoc Networks" ,pp. 1-10 , 2003 https://arxiv.org/abs/cs/0307012

[19] Qi He; Dapeng Wu; P. Khosla "SORI: a secure and objective reputation-based incentive scheme for ad-hoc networks" , IEEE Wireless Communications and Networking Conference (IEEE Cat. No.04TH8733) , 2004 DOI: 10.1109/WCNC.2004.1311293

[20] Tamer Refaei M, Vivek Srivastava, Luiz DaSilva, Mohamed Eltoweissy "A Reputation-based Mechanism for Isolating Selfish Nodes in Ad Hoc Networks" , Vol. 1, Pp.: 3-11 DOI : 10.1109/MOBIQUITOUS.2005.7

[21] Buchegger S, J. -Y. Le Boudee , "Self-policing mobile ad hoc networks by reputation systems", IEEE Communications Magazine , July 2005 , https://doi.org/10.1109/MCOM.2005.1470831

[22] Rekha kaushik and Jyoti Singhai , "DETECTION AND ISOLATION OF RELUCTANT NODES USING REPUTATION BASED SCHEME IN AN AD-HOC NETWORK" , International Journal of Computer Networks & Communications (IJCNC) Vol.3, No.2, pp. 95-105, March 2011

[23] Yu Zhang, Loukas Lazos and William Jr. Kozma , "AMD: Audit-based Misbehavior Detection in Wireless Ad Hoc Networks" , IEEE TRANSACTIONS ON MOBILE COMPUTING, Vol. 15, Issue 8 , 2016

[24] Kejun Liu; Jing Deng; Pramod K. Varshney; Kashyap Balakrishnan , "An Acknowledgment-Based Approach for the Detection of Routing Misbehavior in MANETs" , IEEE Transactions on Mobile Computing , Vol. 6 Issue 5,pp. 536 - 550 May 2007 DOI: 10.1109/TMC.2007.1036

[25] Jamal N. Al-Karaki and Ahmed E. Kamal "Stimulating Node Cooperation in Mobile Ad hoc Networks" , Springer - Wireless Personal Communications , Vol. 44, pp. 219–239 , 2008

[26] Djenouri, Djamel; Badache, Nadjib , "On eliminating packet droppers in MANET: A modular solution" , Elsevier - Ad Hoc Networks , Vol.7 Issue 6, pp. 1243-1258 , 2009 https://doi.org/10.1016/j.adhoc.2008.11.003

[27] Hidehisa Nakayama; Satoshi Kurosawa; Abbas Jamalipour; Yoshiaki Nemoto; Nei Kato, "A Dynamic Anomaly Detection Scheme for AODV-Based Mobile Ad Hoc Networks" , IEEE Transactions on Vehicular Technology Vol. 58 Issue 5 , pp. 2471 – 2481 , Jun 2009 DOI: 10.1109/TVT.2008.2010049

[28] Chengqi Song and Qian Zhang , "COFFEE: A Context-Free Protocol for Stimulating Data Forwarding in Wireless Ad Hoc Networks" , 6th Annual IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks, June 2009 DOI: 10.1109/SAHCN.2009.5168916

[29] Lien-Wen Wu and Rui-Feng Yu , "A threshold-based method for selfish nodes detection in MANET" , IEEE - International Computer Symposium (ICS2010), Dec. 2010 DOI: 10.1109/COMPSYM.2010.5685389

[30] Fatemeh Barani , "A hybrid approach for dynamic intrusion detection in ad hoc networks using genetic algorithm and artificial immune system" , IEEE Iranian Conference on Intelligent Systems (ICIS) , Feb. 2014 DOI: 10.1109/IranianCIS.2014.6802607

[31] Debdutta Barman and RoyRituparna Chaki , "MABHIDS: A New Mobile Agent Based Black Hole Intrusion Detection System", Springer - book series - Communications in Computer and Information Science (CCIS) vol. 245 , pp 85-94

[32] Usha S and Radha S , "Multi Hop Acknowledgement Scheme based Selfish Node Detection in Mobile Ad hoc Networks" , International Journal of Computer and Electrical Engineering (IJCEE), Vol 3 Issue 4, pp. 524-528 Aug. 2011 DOI: 10.7763/IJCEE.2011.V3.373

ISSN: 2233-7857 IJFGCN

[33] Abderrahmane Baadache and Ali Belmehdi ," Fighting against packet dropping misbehavior in multi-hop wireless ad hoc networks" , Journal of Network and Computer Applications , Vol. 35 Issue 3 , pp. 1130–1139 May 2012 https://doi.org/10.1016/j.jnca.2011.12.012

[34] Hussain, M.A , Nadeem A.; Khan, O.; Iqbal, S.; Salam, A., "Evaluating network layer selfish behavior and a method to detect and mitigate its effect in MANETs," Multitopic Conference (INMIC), 2012 15th International, vol., no., pp.283,289, Dec. 2012.

[35] Enrique Hernández-Orallo , Manuel David Serrat Olmos , Juan-Carlos Cano , Carlos T. Calafate and Pietro Manzoni , "CoCoWa: A Collaborative Contact-Based Watchdog for Detecting Selfish Nodes" , IEEE Transactions on Mobile Computing, Vol 14 Issue 6, pp. 1162 – 1175 , June 2015 DOI: 10.1109/TMC.2014.2343627

[36] Aishwarya S. Anand Ukey , Meenu Chawla and Virendra Pal Singh, "I-2ACK: Preventing Routing Misbehavior in Mobile Ad hoc Networks" , International Journal of Computer Applications, Vol. 62 Issue 12, pp. 34 – 39 , 2013 DOI 10.5120/10134-4924

[37] Andreas Lobinger , Szymon Stefanski , Thomas Jansen and Irina Balan , "Coordinating Handover Parameter Optimization and Load Balancing in LTE Self-Optimizing Networks" IEEE 73rd Vehicular Technology Conference (VTC Spring), May 2011 , liuDOI: 10.1109/VETECS.2011.5956561

[38] Latlia Kant and Wai Chen, "Service survivability in wireless networks via multi-layer self-healing" , IEEE Wireless Communications and Networking Conference, March 2005 , DOI: 10.1109/WCNC.2005.1424898

[39] Debdutta Barman Roy and Rituparna Chaki, "MADSN: Mobile Agent Based Detection of Selfish Node in MANET ",International Journal of Wireless & Mobile Networks (IJWMN) Vol. 3, No. 4, pp. 225-235 , August 2011

[40] Xiaohui Liang , Xu Li , Qinghua Shen , Rongxing Lu , Xiaodong Lin , Xuemin Shen and Weihua Zhuang , "Exploiting prediction to enable Secure and Reliable routing in Wireless Body Area Networks" , Proceedings IEEE INFOCOM , March 2012 , DOI: 10.1109/INFCOM.2012.6195777

[41] Mangesh M Ghonge , P. M. Jawandhiya and V. M. Thakare , "Selfish attack detection in mobile Ad hoc networks" , IEEE - International Conference on Innovations in Information, Embedded and Communication Systems (ICIIECS) , March 2017 DOI: 10.1109/ICIIECS.2017.8276136

[42] Sengathir J, & Manoharan R. "A split half reliability coefficient based mathematical model for mitigating selfish nodes in MANETs" , IEEE 3rd International Advance Computing Conference (IACC), pp. 78-87 2013 DOI: 10.1109/IAdCC.2013.6514233

[43] Neenavath Veeraiah and Krishna B. T , "Selfish node detection IDSM based approach using individual master cluster node" , IEEE - 2nd International Conference on Inventive Systems and Control (ICISC) , Jan. 2018 DOI: 10.1109/ICISC.2018.8399109

[44] MOHAMED MUSTHAFA M ,VANITHA K, MD. ZUBAIR RAHMAN A.M.J and ANITHA K, "An Efficient Approach to Identify Selfish Node in MANET" , IEEE - International Conference on Computer Communication and Informatics (ICCCI), Jan 2020 DOI: 10.1109/ICCCI48352.2020.9104076.

[45] Atul Sharma, Dinesh Singh , Poonam Sharma and Sanjeev Dhawan , "Selfish nodes detection in delay tolerant networks" , IEEE -International Conference on Futuristic Trends on Computational Analysis and Knowledge Management (ABLAZE) , Feb. 2015 DOI: 10.1109/ABLAZE.2015.7155030.

ISSN: 2233-7857 IJFGCN