International Journal of Engineering Research in Computer Science and Engineering (IJERCSE) Vol 2, Issue 7, July 2015

An Inspective Approach of Misbehaviour Detection in Wireless Adhoc Networks

[1]N.Velvizhi, [2]Avinashilingam.N, [3] Anith kumar.R
[1] Professor, Department of Computer Science and Engineering,RMD Engineering College,Kavaraipettai,Chennai
[2] Student, Department of Computer Science and Engineering,RMD EngineeringCollege,Kavaraipettai,Chennai,
[3] Student, Department of Computer Science and Engineering,RMD Engineering College,Kavaraipettai,Chennai
601206,Tamil Nadu,India

Abstract: **The goal of this paper is to identify the misbehaving node and isolating its participation from the multi hop ad hoc network. An ad hoc network is a collection of wireless mobile hosts forming temporary network without the aid of any established infrastructure or centralized administration. The selective and continuous packet droppers are effectively and efficiently identified and isolated by the proposed Inspective approach of misbehavior detection in wireless ad hoc network (IAMD). The concept of discovery of routes that is trustworthy along with a reputation management system is incorporated in the proposed inspective approach of misbehavior detection in wireless ad hoc networks (IAMD) method. In comparison with the existing previous techniques, the evaluation of IAMD is done on the basis of a node behavior for per packet excluding the overhearing techniques that consumes energy and also the acknowledgement schemes. IAMD detects selective dropping packets even in encrypted end to end traffic and can be applied to multichannel networks or networks consisting of nodes with directional antennas. The nodes that are misbehaving and even a large portion of network that refuses to forward the packets is detected successfully by IAMD approach and that is effectively proved through simulation**

Index Terms— Wireless **Ad hoc Network, Misbehaving, auditing, packet dropper, and Reputation value.**

I. INTRODUCTION

A supporting infrastructure is absent in wireless ad hoc networks and this gives rise to the need realizing the importance of end to end communication in a co-operative manner. The finite communication range leads the nodes to find multi hop routes. Therefore from source to destination the intermediate nodes also become responsible in relaying the packets. In mobile ad-hoc networks, nodes are both routers and terminals. For lack of routing infrastructure, they have to cooperate to communicate. Cooperation at the network layer means routing, i.e., finding a path for a packet, and

forwarding, i.e., relaying packets for others. Misbehavior means deviation from regular routing and forwarding. It arises for several reasons, non-

intentionally when a node is faulty; Intentional misbehavior can aim at an advantage for the misbehaving node or just constitute vandalism, such as enabling a malicious node to mount an attack or a selfish node to save power. Economic incentives such as payment schemes aim at making selfish nodes forward for others despite the power usage and effort this entails. Nodes are paid for forwarding and pay for the forwarding of their own packets by other nodes. An example is neglects, a virtual currency, or the credit counter, where nodes keep track of remaining battery power and credit. These approaches make it undesirable for selfish nodes to deny forwarding. They do not, however, target other types of misbehavior. Secure routing and economic incentives solve part of the question, but not all. There remains a variety of observable types of misbehavior that they cannot cure easily, such as silent route changes, which may be addressed by detection and reputation systems. They monitor and rate the behavior of other nodes in routing and forwarding, such that nodes can respond according to their opinion about other nodes.

This work proposes to show a complete technique IAMD (Inspective approach of misbehavior detection in wireless ad hoc network) to detect and isolate a misbehavior node and also ensure a trustworthy route for a data transfer from source to destination. IAMD can construct paths consisting of highly trusted nodes, subject to a desired path length constraint. When paths contain misbehaving nodes, these nodes are efficiently

located by a behavioral audit process. The IAMD system integrates reputation management, trustworthy route discovery, and identification of misbehaving nodes based on behavioral audits. Compared to previous methods, IAMD evaluates node behavior on a per-packet basis, without employing energy-expensive overhearing techniques or intensive acknowledgment schemes.

II. RELATED WORK

In wireless ad hoc network node misbehavior due to selfish or malicious reasons or faulty nodes can significantly degrade the performance of mobile ad hoc networks. Sonja Buchegger , Jean-Yves Le Boudec . [1] proposed a scheme in which they says that to cope with misbehavior in such self-organized networks, nodes need to be able to automatically adapt their strategy to changing levels of cooperation. Existing approaches such as economic incentives or secure routing by cryptography alleviate some of the problems, but not all. We describe the use of a self-policing mechanism based on reputation to enable mobile ad-hoc networks to keep functioning despite the presence of misbehaving nodes. The reputation system in all nodes makes them detect misbehavior locally by observation and use of second-hand information. Once a misbehaving node is detected it is automatically isolated from the network. We classify the features of such reputation systems and describe possible implementations of each of them. We explain in particular how it is possible to use second-hand information while mitigating contamination by spurious ratings.

This work has proposed a detection and reputation systems called as CONFIDANT. Nodes monitor their neighborhood and detect several kinds of misbehavior; by means of an enhanced passive acknowledgment mechanism. The reputation system is not effective when the number of misbehaving nodes is too large.

Sergio Marti, T.J. Giuli, Kevin Lai, and Mary Baker. [2] Developed two techniques that improve throughput in an ad hoc network in the presence of nodes that agree to forward packets but fail to do so. To mitigate this problem, we propose categorizing nodes based upon their dynamically measured behavior. We use a watchdog that identifies misbehaving nodes and a path rater that helps routing protocols avoid these nodes. Through simulation we evaluate watchdog and path rater using packet throughput, percentage of overhead (routing) transmissions, and the accuracy of misbehaving node detection. When used together in a network with moderate mobility, the two techniques increase throughput by 17% in the presence of 40% Misbehaving nodes, while increasing the percentage of overhead transmissions from the standard routing protocol's 9% to 17%. During extreme mobility, watchdog and path rater can increase network throughput by 27%, while increasing the overhead transmissions from the standard routing protocol's 12% to 24%.DSR with the watchdog has the advantage that it can detect misbehavior at the forwarding level and not just the link level. Watchdog's weaknesses are that it might not detect a misbehaving node in the presence of Ambiguous collisions, Receiver collision, Limited transmission power, false misbehavior, Collusion and Partial dropping

In a multi-hop wireless ad hoc network, packet losses are attributed to harsh channel conditions and intentional packet discard by malicious nodes. Tao Shu and Marwan Krunz. [3] Proposed sprite, in this while observing a sequence of packet losses, we are interested in determining whether losses are due to link errors only, or due to the combined effect of link errors and malicious drop. We are especially interested in insider's attacks, whereby a malicious node that is part of the route exploits its knowledge of the communication context to selectively drop a small number of packets that are critical to network performance. Because the packet dropping rate in this case is comparable to the channel error rate, conventional algorithms that are based on detecting the packet loss rate cannot achieve satisfactory detection accuracy. To improve the detection accuracy, we propose to exploit the correlations between lost packets. Furthermore, to ensure truthful calculation of these correlations, we develop a homomorphism linear authenticator (HLA) based public auditing architecture that allows the detector to verify the truthfulness of the packet loss information reported by nodes. This architecture is privacy preserving, collusion proof, and incurs low communication and storage overheads. Through extensive simulations, we verify that the proposed mechanism achieves significantly better detection accuracy than conventional methods such as a maximum-likelihood based detection. Exploiting the correlation between lost packets significantly improves the accuracy in detecting malicious packet drops HLA-based public auditing architecture that ensures truthful packet-loss reporting by individual nodes. This architecture is collusion proof. The HLA-based public auditing architecture requires relatively high computational capacity at the source node, but incurs low communication and storage overheads over the

route. The computational overhead at source nodes needs to be reduced. This work explores a model for the operation of an ad hoc mobile network. Jon Crow croft, Richard Gibbens, Frank Kellyz, Sven Ostring. [4] Proposed a model that incorporates incentives for users to act as transit nodes on multi-hop paths and to be rewarded with their own ability to send traffic. The work explores consequences of the model by means of fluid-level simulations of a network and illustrates the way in which network resources are allocated to users according to their geographical position. In this work, we specifically consider the issue of how prices can be determined automatically by the ability of nodes to pay the costs for transmitting traffic, and the routes that are subsequently used. We show that cooperation is a natural outcome that emerges from incentives created by the pricing mechanisms. We further study the way that the mobility of the users affects system performance. The fluid-level simulations shows that users prices and credit balances stabilize for a static ad hoc network and shown the advantages in being near the centre of the network, as this allows nodes to act as transit nodes for a larger number of routes. The mobility through the centre of the network can increase an individual user's throughput, as well as increase the overall throughput of the system is revealed in this work.

The traditional approach of providing network security has been to borrow tools from cryptography and authentication. However, we argue that the conventional view of security based on cryptography alone is not sufficient for the unique characteristics and novel misbehaviors encountered in sensor networks. Fundamental to this is the observation that cryptography cannot prevent malicious or non-malicious insertion of data from internal adversaries or faulty nodes. We believe that in general tools from different domains such as economics, statistics and data analysis will have to be combined with cryptography for the development of trustworthy sensor networks. Following this approach Saurabh Ganeriwal and Mani B. Srivastava. [5] Propose a reputation-based framework for sensor networks where nodes maintain reputation for other nodes and use it to evaluate their trustworthiness. We will show that this framework provides a scalable, diverse and a generalized approach for countering all types of misbehavior resulting from malicious and faulty nodes. We are currently developing a system within this framework where we employ a Bayesian formulation, specifically a beta reputation system, for reputation representation, updates and integration. We will explain the reasoning behind our design choices, analyzing their pros & cons. We conclude the work by verifying the efficacy of this system through some preliminary simulation results. All types of misbehavior resulting from malicious and faulty nodes are countered by a reputation-based framework for sensor networks where nodes maintain reputation for other nodes and use it to evaluate their trustworthiness.

Internet routing is vulnerable to disruptions caused by malfunctioning or malicious routers that draw traffic towards them but fail to correctly forward the traffic. The existing approach to securing routing is to validate routing updates by verifying their authenticity, accuracy, and/or consistency. The key idea behind secure trace route is to securely trace the path of existing traffic, rather than that of special trace route packets, to prevent adversaries from misleading the tracer by treating trace route and normal traffic differently. Secure trace route responses are also authenticated, to verify their origin and prevent spoofing or tampering. Venkata N. Padmanabhan and Daniel R. Simon. [6] Propose a different, adaptive approach, the central idea of which is a secure Trace route protocol that enables end hosts or routers to identify an arbitrarily severely misbehaving router, so that appropriate action can be taken. Routers, assisted by end hosts, adaptively detect poorly performing routes that appear suspicious, and use a secure trace route protocol to attempt to detect an offending router. This approach complements efforts that focus on securing the routing protocol itself, secure trace route as a general technique with wide applicability is viewed.

S. A. Razak, S. M. Furnell, P. J. Brooke. [7] Proposed some important issues that relate to security attacks against mobile ad hoc networks from research carried out at Network Research Group, University of Plymouth, on designing intrusion detection system for mobile ad hoc network. In designing security mechanisms for mobile ad hoc networks, one must consider the attacks variations as well as the characteristics of the attacks that could be launched against the ad hoc networks. The discussions of these two aspects are summarized in this work. This work also classifies several common attacks against the ad hoc networks routing protocols based upon the techniques that could be used by attackers to exploit routing messages. Those techniques are modification, interception, fabrication, and interruption. This work has identified that most of the attacks against ad hoc networks routing protocols are actually launched by

exploiting the routing messages, and has further classified them based upon the techniques that could be used to exploit routing messages. Techniques that involves protecting, detecting, and responding to the attacks against the routing messages is not more emphasized.

Internet is a global network where it is easily prone to be attacked by hackers. Packet loss exhibits temporal dependency. Many approaches have been implemented to provide secure route for the packets sent and finding out malicious packets. Julian Benadit.P, Sharmila Baskaran and Ramya Taimanessamy[8]. Proposed a system that use a protocol and maintain log at each router to find out where the loss actually occurred. Our paper mainly focuses on where the packet has dropped or attacked. In this paper, we propose an operationally viable approach to find out where the loss occurred. If an attacker gains control over a router, he could disrupt the communication by dropping or manipulating the packets sent. Traffic can be severely disrupted by routers refusing to serve their advertised routes, announcing nonexistent routes, or simply failing to withdraw failed routes, as a result of either malfunction or malice. The key idea behind detecting malicious packet loss is finding where the packet loss has occurred in the network using a protocol and maintaining log. The attackers may disrupt packet forwarding (i.e., the data plane of the network) by dropping packets routed to it by its neighbors. Authentication of the routing protocol messages is not sufficient to prevent the disruption of routing. Even though the Border Gateway Routing Protocol (BGP) [6] is central for Internet packet routing, it was designed for a trusted environment and provides relatively minimal security against an attacker. We need a way to securely detect and localize the source of packet forwarding misbehavior so that the problem can then be corrected by routing around the trouble spot.

III. PROBLEM DEFINITION

In a deployment of a network a portion of it is assumed to be misbehaving. This misbehavior is marked by the dropping of transit traffic from a source to a destination. Misbehaving nodes can be continuous droppers, or adopt any selective dropping strategy. When a path with a source to destination of a particular length which consists of a number of misbehaving nodes is considered, the number of misbehaving nodes must be equal or less than the length of nodes along the path. The other types of misbehavior against the routing process such as advertisement of false routing information, creation of sinkholes, black holes, wormholes is not considered in this work. The selfish node behavior is also not emphasized in this work since it already isolates itself from transmissions involved for other nodes. This work henceforth deals with route discovery that must trustworthy. The misbehaving nodes along the path of source to destination must be identified and thus discover a route that is free from such misbehaving nodes and consequently ensure a trustworthy data delivery from source to destination. This problem of identifying and isolating misbehaving nodes that refuse to forward packets in multi-hop ad hoc networks is dealt in this work.

IV. SYSTEM OVERVIEW

WIRELESS ADHOC NETWORK ARCHITECTURE

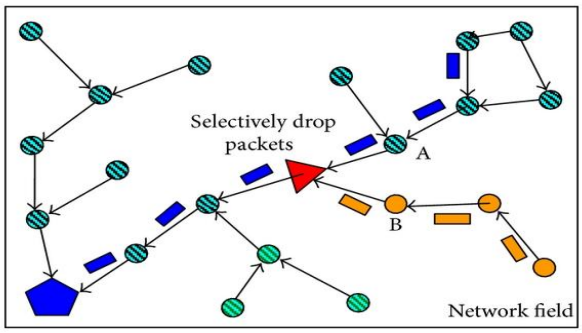


Fig 1: Example of wireless ad hoc network

In a multi-hop wireless ad hoc network, packet losses are attributed to harsh channel conditions and intentional packet discard by malicious nodes. When a sequence of packet losses are observed, an examining has to be done whether losses are due to link errors only, or due to the combined effect of link errors and malicious drop. In the absence of a supporting infrastructure, wireless ad hoc networks realize end-to-end communications in a cooperative manner. Nodes rely on the establishment of multi-hop routes to overcome the limitations of their finite communication range. In this paradigm, intermediate nodes are responsible for relaying packets from the source to the destination. The network model presupposes that intermediate nodes are willing to carry traffic other than their own. When ad hoc networks are deployed in hostile environments (tactical networks), or consist of nodes that belong to multiple independent entities, a protocol-compliant behavior cannot be assumed. Unattended devices can become compromised and drop transit traffic in order

to degrade the network performance. Moreover, selfish users may misconfigure their devices to refuse forwarding traffic in order to conserve energy. This type of behavior is typically termed as node misbehavior.

This work aims at showing an inclusive technique for identifying the misbehaving node and isolating its participation from the multi hop ad hoc network. The selective and continuous packet droppers are effectively and efficiently identified and isolated by the proposed Inspective approach of misbehavior detection in wireless ad hoc network (IAMD).

A network architecture that is multi hop is considered. The path from source to destination is defined. When a route is established through trace route operation the path from source to destination can be identified. It is assumed that even a source can monitor the path of a route from source to destination. The identification of a misbehaving node for the establishment of a trust based route from source to destination that which does not contain any misbehaving node is proposed in this work.

A fraction of the nodes deployed in the network is assumed to be misbehaving. This misbehavior is made clear by the dropping of transit traffic from a source to a destination. The misbehavior that is shown in this work involves of two types of sort. The misbehaving node must either be a continuous dropper or it must possess a selective dropping strategy so it cannot be that easily and in the early hours identified as a misbehaving node. A path is considered to have a particular length that the number of hops or the number of nodes it travels to complete the path along the route. It is assumed that the number of misbehaving nodes is either less than or equal to the number of nodes along its length.

REPUTATION BASED SYSTEM

The reputation based system is considered in the proposed work. Each node maintains its own view of reputation value about the other nodes in the network. The nodes that contain a low reputation value are excluded from the specified routing path. The reputation section in the proposed structure does the work of computation and management of all the reputation that is involved in the network. Two types of information considering is done for the implementation of reputation system.

- First hand information
- Second hand information

First-hand information is obtained by direct interaction between nodes that is from the nodes that belong to the path from source to destination.

Second-hand information is indirectly obtained based on the opinions of other nodes.

The computation of reputation values is done based on the above two criteria. A multi hop network consists of a number of nodes wherein within a particular time period the reputation values for every node is computed. The range of the reputation values fall within the range 0-1.

The first hand information technique is based on AIMD (Additive increase/multiplicative decrease) algorithm from which the misbehavior of a node is determined.

Second hand information is adopted when first hand information is stale. Here, any one node among all that belong to the path of source to destination averages all information reported by the other nodes within the specified time period for reputation.

THE PROCESS OF ROUTE DISCOVERY

The route discovery process is responsible for the discovery of trustworthy paths from a source to a destination. This module is invoked by the source whenever there is no cached path to the destination. A path from source to destination *can* be seen as an in-series system of independent components. The failure of one component i.e., a node dropping packets results in the failure of the entire path or even the system. The reliability of in-series systems is defined as the product of the reliability values of the individual components. Analogous, to this the trustworthiness of a path is defined as the product of the reputation values of the nodes that participate in that path.

A fine point in this definition is the fact that there is no universal reputation value for each node, but the reputation values are individual perceptions of trustworthiness of one node in regards to another.

Hence, to compute the path reputation value, the reputation values along the path of intermediate nodes as perceived by all the nodes participating as in from source to destination. Hence, a malicious node with low reputation value cannot increase the path reputation to a value higher than its own reputation. A malicious node can, however, lower the reputation value of a path by lying about the reputation values of other nodes. This strategy decreases the path reputation, leading to the exclusion of the lying node from routing paths.

THE PROPOSED SCHEME- INSPECTIVE APPROACH OF MISBEHAVIOUR DETECTION (IAMD)

The proposed scheme introduces a complete technique that helps in the identification of the misbehaving node with successful elimination from the network. The IAMD system architecture consists of three modules.

- Reputation module
- Route discovery module
- Audit module

Each of these three modules contributes a specific function from which all co-ordinates to perform the process of misbehavior detection, discovery of trustworthy routes, and evaluation of the reputation of peers.

The reputation module is responsible for managing reputation information based on the recommendations of the audit module. Reputation values are exploited by the route discovery module for establishing routes that exclude nodes with low reputations.

The audit module efficiently identifies misbehaving nodes through an audit process. This process is accelerated based on the input that is received from the reputation module.

When poor performance is detected over the path of source to destination the source requests from a subset of intermediate nodes to record a digest of the set of packets they forward to the next hop. This is termed as the audit process. Although misbehaving nodes can lie when audited, audit replies from honest nodes lead to the identification of those lies, and eventually of the misbehaving nodes.

The audit module is responsible for identifying the set of nodes that misbehave in a particular path. The source invokes the audit module if it detects poor performance on the path from source to destination. The exact definition of what constitutes poor performance can be determined on the basis of a specific application running between source *and* destination. One possible mechanism for determining the path performance is to monitor the average end-to-end packet rate over a window of time‘t’. When the end-to-end packet rate is less than a specified threshold, the audit module is activated. The threshold is source-defined and can be statistically derived based on prior interactions of the source with other destinations, or some minimum expected network performance. The rate can be calculated at the source *either* by taking into account transport layer end-to-end acknowledgements, or explicit feedback provided periodically by destination. When poor performance is detected over path, the source requests from a subset of intermediate nodes to record a digest of the set of packets they forward to the next hop. This is called as the audit process. Although misbehaving nodes can lie when audited, audit replies from honest nodes lead to the identification of those lies, and eventually of the misbehaving nodes.

The audit process occurs in three steps:

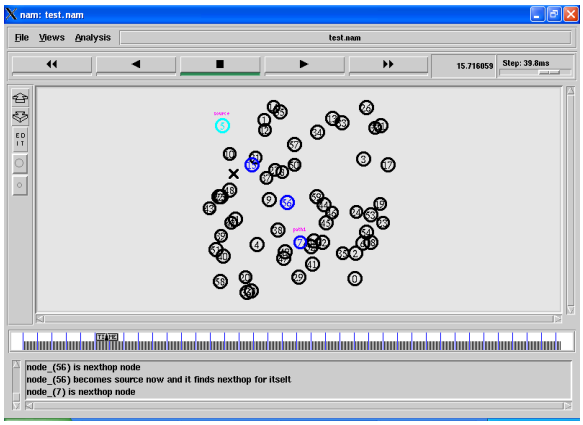
- Sending an audit request
- Constructing an audit reply
- Computing the audit claim

PERFORMANCE EVALUATION

It is observed that the reputation value of malicious nodes rapidly decreases with the progress of time. On the other hand, the reputation value of honest nodes progressively approaches the maximum value of one. During the comparison of the performance of IAMD with the performance of DSR in the percentage of dropped packets due to misbehavior IAMD quickly reduces the percentage of dropped packets to almost zero. This is due to the fact that misbehaving nodes are excluded from the routing paths as their reputation value decreases. Hence, most routes consist only of honest nodes. A further implementation was done on a random packet dropping behavior in which misbehaving nodes randomly dropped a fraction of the traffic as a function of time when 20% of the nodes are misbehaving. It is observed that a less aggressive behavior can only delay the isolation of misbehaving nodes. Therefore, the proposed work has thus proved to be efficient in identifying the node with malicious behavior and thus reveals its work effective isolation of that node through audit based process.

V. EXPERIMENTAL RESULT

Here we have deployed the network with 60 nodes in which we assumed that node 5 is source and node 7 is destination and found the trustworthy route based on the history of transactions.



S.no	Source	Destination	Avg no.of Packets Delivered (in %)	Avg No.of Packets Missed during communication (in %)
1	4	7	69.08	22.45
2	5	13	72.62	23.00
3	2	8	73.03	21.25

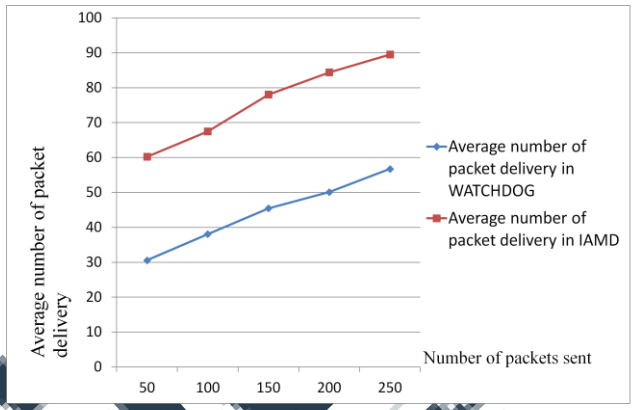
In this we have considered three paths through which the packets are forwarded from source to destination. The path which contains high reputation will forwards the packet efficiently without any loss of packets that is considered as secured path.

TABLE2: COMPARISON OF PACKET DELIVERY (WATCHDOG AND IAMD)

s.no	No.of Packets Sent	Avg No.of Packet Delivery in Watch Dog(in %)	Avg No.of Packet Delivery In IAMD (in %)
1	50	40.28	78.23
2	100	41.05	79.41
3	150	40.55	77.80
4	200	39.48	80.12
5	250	39.04	79.88

Figure.2 shows the comparative results of WATCHDOG and IAMD, where x-axis indicates the number of packets sent and y-axis represents average number of packet delivery in percentage. The graph shows that the average number of packet delivery in

IAMD is maximized about 40 percent compared to WATCHDOG. In the figure.2, we can see that the overall performance of IAMD is increased dynamically compared to WATCHDOG.



VI. CONCLUSION AND FUTURE WORK

In this work the identification and isolation of node with malicious behavior was proposed. The malicious behavior emphasized in this work deals with the node that drops packets continuously or nodes that adapts a specific strategy for selective dropping. A comprehensive technique called IAMD (Inspective approach of misbehavior detection in wireless ad hoc network) is proposed to effectively identify and isolate the node with misbehavior from the link and thus provide way for the establishment of a trustworthy path that does not contain misbehaving nodes. The IAMD technique proposed in this work integrates three factors

- Reputation management
- Route discovery
- Identification of misbehaving nodes through behavioral audits

The effectiveness of IAMD is proved wherein even when a larger area of network is misbehaving at a lower cost the IAMD scheme is able to detect the misbehaving node.Further this system can be enhanced with Rate Limiting technique which can be used to control the rate of traffic sent or received by a Network Interface Controller.

REFERENCES

[1] Sonja Buchegger, Jean-Yves Le Boudec, "Self-Policing Mobile Ad-Hoc Networks by Reputation Systems". IEEE Comm. Magazine, pp 101–107, 2005.

[2] Jon Crowcroft, Richard Gibbens, Frank Kellyz, Sven Ostring, " Modeling Incentives forCollaboration in Mobile Ad Hoc Networks". In Proc. of WoWMoM, pp 1–6, 2010.
[3] Y. Dong, H. Go, A. Sui, V. Li, L. Hui, and S. Yiu. Providing distributed certificate authority service in mobile ad hoc networks. In Proc. Of SecureComm 2005, pp 149–156, 2005
\

[4] L. M. Feeney and M. Nilsson. "Investigating the energy consumption of a wireless network interface in an ad hoc networking environment". In Proc.of INFOCOM, pp 1548–1557, 2001
[5] Saurabh Ganeriwal and Mani B. Srivastava, "Reputation-based Framework for High Integrity Sensor Networks". ACM Transctions on Sensor Network s,4(3):1–37, 2008.
[6] Q. He, D. Wu, and P. Khosla."A secure and objective reputation-based incentive scheme for ad hoc networks". In Proc. of WCNC, 2004.
[7] W. Kozma Jr. and L. Lazos. "Resource-efficient accountability for node misbehavior in ad hoc networks based on random audits". In Proc. of WiSec, 2009.
[8] Sergio Marti, T.J. Giuli, Kevin Lai, and Mary Baker, "Mitigating Routing Misbehavior in Mobile Ad Hoc Networks". In Proc. of MobiCom, pp 255–265, 2000.
[9] P. Misheard and R. Molva. CORE: a collaborative reputation mechanism to enforce node cooperation in mobile ad hoc networks. In Proc. of CMS, pp 107–121, 2002.
[10] Venkata N. Padmanabhan and Daniel R. Simon,"Secure Traceroute to Detect Faulty or Malicious Routing". SIGCOMM CCR, 33(1), 2003
[11] S. A. Razak, S. M. Furnell, P. J. Brooke, "Attacks against Mobile Ad Hoc Networks Routing Protocols"
[12] Tao Shu and Marwan Krunz, "Detection of Malicious Packet Dropping in Wireless Ad Hoc Networks Based on Privacy-Preserving Public Auditing". In Proc.of WiSec, pp 87–98, 2012
[13] Alper Tugay Mızrak, Keith Marzullo, Stefan Savage"Fault-Tolerant Forwarding in the Face of Malicious Routers". Wireless Personal Communications, Special Issue on Security for Next Generation Communications, 29(3-4):367–388, 2004.