Mitigating Selfish Behavior in Mobile Ad Hoc Networks: A Survey

Mani P.
Department of MCA,
M. Kumarasamy College of Engineering, Karur,
India.

Kamalakkannan P.
PG and Research Department of Computer
Science
Government Arts College (Autonomous)
Salem, India.

ABSTRACT

Mobile Ad hoc Networks (MANETs) is a collection of mobile nodes forming the network dynamically for exchange of information using the multi-hop wireless communications without the need of any pre-existing infrastructure. The mobile nodes act as hosts as well as router to establish communication among nodes in the network. To achieve high throughput nodes are expected to cooperate with each other in packet forwarding process to enable out of range communication. In MANETs, all the routing protocols are designed with an assumption that the nodes will cooperate in packet forwarding. But the inherent characteristics of MANETs such as no fixed infrastructure, dynamic topology, limited battery power and wireless medium introduces node misbehavior. An individual node may behave selfishly to preserve its scarce resources and do not forward the packets to other nodes but still want to use their services to send and receive their own packets. The selfish behavior affects the performance of the network significantly. Many solutions have been proposed by the researchers to mitigate this selfish behavior. In this paper, we review some of the notable works carried out in mitigating selfish behavior on packet forwarding at the network layer, providing a comprehensive comparison between the different proposed methods.

General Terms

Ad hoc Networks, Selfish Behavior, Packet Forwarding, Mobile Nodes, Mitigating

Keywords

Ad hoc Networks, Selfish Behavior, Packet Forwarding, Mobile Nodes, Mitigating

1. INTRODUCTION

Mobile Ad Hoc Networks is a collection of mobile nodes which are formed on the move without the need for any basic infrastructure. The communication between the mobile nodes can be established by forwarding the packets over multi-hop wireless links. The MANETs are used in various areas like crisis management and civilian applications. The crisis management includes deployment of mobile nodes in battlefields, emergency search and rescue and law enforcement. The civilian applications includes enabling communication among independent mobile nodes in conference halls, malls etc. In the former application, the mobile nodes are deployed to achieve a common goal whereas in the later, the nodes are belonging to the different group of people. So we cannot expect all the nodes to cooperate with each other for packet forwarding. Some of the nodes do not wish to forward the packets in order to save its own resources like battery power, computational power and bandwidth. But still they want to use the services of other nodes to send and receive their own packets.

Inherent characteristics of MANETs, like no fixed infrastructure, wireless medium and dynamic topology, introduces various security attacks. These attacks can be broadly classified into two categories namely passive and active attacks. In passive attacks, the misbehaving nodes do not disturb the operation of the network, but it collects the needed information about the network since it is very difficult to find out the passive attack. An active attack disturbs the operation of the network and can further be classified into internal attacks and external attacks. The internal attacks are launched by the nodes which are part of the network whereas the external attacks are launched by the nodes which are not part of the network.

In order to combat passive and active attacks, MANETs are expected to satisfy the following security requirements.

1.1 Security Requirements

1.1.1 Confidentiality

The network should ensure that the given message cannot be understood by anyone other than its recipients. It can be enabled by cryptographic technique.

1.1.2 Authentication

The network should ensure that the data is sent and received by the authenticated user only.

1.1.3 Non-Repudiation

It is the ability of the network to ensure that a node cannot deny the sending of a message that it originated.

1.1.4 Availability

The network should provide the required services to the authenticated users when it is expected.

1.1.5 Integrity

The system should ensure that the message sent from the sender is received by the receiver without any modification during transmission.

1.2 Security Issues in Packet Forwarding

Protecting the network layer in MANETs is a highly important research topic. There are two main network layer operations in mobile ad hoc networks [1] [2].

- Routing
- Packet Forwarding

The mobile nodes interact with other for delivering packets from source to destination. The main function of the ad hoc routing protocols is to provide routing among nodes. They exchange routing messages between different mobile nodes in order to maintain routing information at each node. The data forwarding service consists of correctly relaying the received packets from node to node until they reach their final destination, following the routes selected and maintained by the routing protocol. Both of these applications are vulnerable to malicious attacks, which will lead to various types of malfunction in network layer.

1.2.1 Data forwarding threats

1.2.1.1 Eavesdropping

The wireless channels used in MANETs are freely and easily accessible. Some of the routing protocols may use the promiscuous mode to learn routes and these features can be exploited by malicious nodes eavesdrop packets in transit, and then analyze them to obtain confidential and sensitive information. One solution to protect information is to encrypt packets, but data encryption does not prevent malicious nodes from eavesdropping and trying to break decryption keys.

1.2.1.2 Dropping data packets attack

The communication between the mobile nodes can be established by forwarding the packets over multi-hop wireless links. The malicious node first attack the routing protocol to join in the routing path and it starts dropping the packets expected to be relayed in order to disrupt the network layer functions.

1.2.2 Selfish behavior on packet forwarding

In many civilian applications the nodes does not belong to a single authority and do not have a common goal. In such networks, forwarding packets for others is not in the direct interest of nodes, so there is no good reason to trust nodes and assume that they always cooperate. Indeed, a selfish node may try to preserve its resource. This is not an intentional attack but a selfish behavior. The selfish nodes are rational in that they want to leverage the other node in the network to send and receive whereas the nodes with malicious behavior aim to disturb other nodes but not to save their own resources. This paper discusses various methods proposed to combat the selfish behavior in MANETs and is structured as follows: Section 2 addresses the various methods proposed to mitigate the selfish misbehavior and section 3 concludes the paper.

2. MITIGATING SELFISH BEHAVIOR

Most of the works to mitigate selfish behavior can be classified into Incentive-Based Mechanism, Reputation-Based Mechanism and other mechanisms. The trust models based on certification-based category are surveyed in the literature by M.Omar[3]. 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 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.

2.1 Incentive-based Mechanisms

2.1.1 Virtual Currency

One of the most reputable works in this category is the nuglets proposed in [4]. 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.

The packet forwarding service presents three charging models. In this charging model, the nuglets are represented by counters in the nodes. Each node has a nuglet counter and it is maintained by a trusted and tamper resistant hardware module in each node called security module. The nuglets are protected from illegitimate modification and detachment from its original packet by cryptographic mechanisms.

Packet Purse Model (PPM), Packet Trade Model (PTM) and a hybrid solution. In packet purse model, the source pays for the forwarding service. The service charge is distributed among the forwarding nodes depending on the amount of energy spent for forwarding, battery status and the number of nuglets. It is the responsibility of the source to load the packets with sufficient number of nuglets otherwise the packets will be dropped before reaching the destination. The advantage of this model is that it avoids nodes from sending useless data and overloading the network. The main drawback of this model is that the packets may be dropped if the source is unable to calculate the correct number nuglets required for transmission.

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. This model also reduces the packet dropping for the want of nuglets. The drawback of this model is that the approach for charging does not directly deter nodes from overloading the network.

The hybrid model combines the advantages of both the models and achieves efficiency in packet forwarding.

2.1.2 Stimulating Cooperation

L. Buttyan in [5] addressed the problem of stimulating cooperation in self-organizing mobile ad hoc networks for civilian applications. 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.

2.1.3 Sprite

In [6], the authors 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 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, even when a collection of nodes collude.

2.1.4 Secure Incentive Protocol

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 in [7]. 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. Each node imprints a non-forged "stamp" on each packet forwarded as the proof of forwarding, based on which packet relays are remunerated, while packet sources and destinations are charged with appropriate credits. 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 SIP designed to be efficient and light weight protocol which can withstand a wide range of cheating attacks and is also of low communication overhead by using bloom filter.

2.1.5 FESCIM

In [8], the authors proposed a fair, efficient and secure cooperation incentive mechanism for multihop 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. To reduce the overhead involved in implementing fairness, the light weight hashing operators are used in ack packets to reduce the number of public key cryptography operations.

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, atleast 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 demonstrated that the overall increase in performance and fairness with the help of hashing operations. This method does not identify the selfishness nodes in the route path.

2.2 Reputation-Based Mechanism

2.2.1 Watchdog and Pathrater

Sergio Marti et al have proposed a method for categorizing nodes based upon their dynamically measured behavior in [9]. The authors have introduced two extensions to the Dynamic Source Routing [10] 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.

The watchdog mechanism is implemented on top of DSR by maintaining a buffer of recently sent packets and comparing each overheard packet with the packet in the buffer to see if there is a match. If so, the packet in the buffer is removed otherwise it determines that the node is misbehaving. The watchdog mechanism works well on top of the source routing protocol. The main drawback of this method is that it may not detect misbehaving nodes in the presence of ambiguous collisions, receiver collisions, limited transmission power, false misbehavior collusion and partial dropping.

2.2.2 CORE

CORE [11] 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 entity's 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) and a Watchdog Mechanism (WD). The CORE scheme uses two types of protocol entities, a requestor and one or more providers. A requestor is a network entity which asks for the execution of a function f and the provider is any entity to correctly execute f.

CORE does not allow a node to distribute negative ratings about other nodes and can resist to simple denial of service attacks that use the security mechanism itself.

2.2.3 CONFIDANT

In [12], the authors have proposed a CONFIDANT protocol 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. The recipients of these ALARM messages are so-called friends. Incoming ALARMs originate from either outside friends or other nodes, so the source of an ALARM has to be checked for trustworthiness before triggering a reaction, thus there is a filtering of incoming ALARM messages according to the trust level of the reporting node.

Here the nodes with a bad reputation may see their requests ignored by the remaining participants, which in practice excludes the node from the network.

2.2.4 SORI

In [13], a Secure and Objective Reputation-based Incentive framework for mobile ad hoc networks is proposed, 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-way- hash chain based authentication scheme and the reputation of a node is only propagated to neighbors which reduces the communication overhead

2.2.5 Reputation-Based

In [14], the authors have proposed a reputation-based mechanism to detect and isolate the selfish nodes. 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. Each node determines whether to forward or drop a packet based on the reputation of the packets previous hop. If the reputation index falls below a pre-determined threshold all the packets are discarded and the node is isolated.

The reputation function is classified into Double Decrement / Single Decrement ratio (DDSIR), Hops Away From Source (HAFS) and Random Early Protection (REP).

In DDSIR, for each successfully delivered packet, a node increment the reputation index by n where n is a positive constant. For each failed delivery, node decrements the reputation index by 2n. The HAFS scheme decrements the reputation index of a neighbor as a function of the number hops between the source and the failed node. The reputation index of a node nearer to the failed node is decremented the most. This reputation function is more aggressive than DDSIR.

The REP scheme is similar to DDSIR. Additionally, a node randomly rejects participation in a route with neighbors whose reputation is r_0 and r_{thresh}. This solution isolates the selfish nodes in an ad hoc network and this method of isolation is more robust because the reputation index of the nodes is not exchanged among the nodes. This method also avoids collusion attack as the reputation mechanism relies primarily on assessing reputation based on direct interaction with other nodes.

2.2.6 Friends and Foes

In Friends and Foes [15], 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 friends are the set of nodes to which node is willing to provide services. The foes are the set of nodes to which node is not willing to provide services and selfish variable gives the list of nodes which are known to act as if node is a foe.

As it introduces "justified selfishness" that makes the whole system more fair not penalizing users by their physical location.

2.2.7 Self-Policing Mobile Ad Hoc Networks by Reputation Systems

In [16], self-policing mechanism 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.

2.3 Other Mechanisms

2.3.1 On eliminating packet droppers in MANETs

Authors have proposed a new solution to monitor, detect, and safely isolate misbehaving nodes that do not forward packets that aims at improving the efficiency in detecting and isolating misbehaving nodes with a minimum overhead in [17]. 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. This approach does not consider the reintegration of isolated nodes and collusive misbehavior.

2.3.2 An acknowledgement-based Approach

In [18], the 2ACK scheme that serves as an add-on technique for routing schemes to detect misbehaving links and to mitigate their adverse effect has proposed. 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 2ACK scheme requires an explicit acknowledgement to be sent by N3 to notify N1 of its successful reception of a data packet. This technique overcomes several problems including ambiguous collisions, receiver collisions, and limited transmission powers. It is more difficult to decide the behavior of a single node.

2.3.3 Stimulating node cooperation in MANETs

The combinations of reputation and incentive-based mechanism have proposed in [19]. 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.

2.3.4 One More Hop

One More Hop protocol is proposed in [20] to suppress the selfish behavior by using the longer path mechanism so that the destination node is no longer fixed as the last hop but can be any intermediate hop. The underlying assumption is that if a node does not know whether the packet it received is destined to itself or not, it cannot drop the packet. Instead of trying to isolate and remove selfish nodes from route path, OMH forces selfish nodes to work normally and makes use of the selfish nodes to forward packets. The OMH protocol encrypts packets, makes the real destination of a packet not equal to the last hop of route path, and gives nodes acknowledgements from its next hop if the node is the real destination.

2.3.5 COFFEE Protocol

In [21], the authors have proposed context-free (COFFEE) protocol 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 COFFEE protocol is having many added features compared to the other methods like resistance to collusion, makes use of selfish nodes and does not need any extra information to work. The computational cost of this protocol is mainly caused by cryptographic processes.

2.3.6 ICARUS

A hybrid incentive mechanism have proposed in [22] combines the advantages of both reputation-based and incentive-based mechanisms in order to detect and punish selfish nodes efficiently and at the same time motivate nodes to cooperate by rewarding the packet forwarding. This method ensures fairness for distant nodes and prevents selfish nodes from corrupting the system using false information.

2.3.7 Fighting Against Packet Dropping

In [23], the authors have proposed a merkle tree principle to verify the correct forwarding of packets by intermediate nodes. This method eliminates the route with packet droppers. The core idea is that all intermediate modes need to acknowledge the reception of packets. Using these acknowledgements, the source node constructs a merkle tree and compares the value of the tree root with a recalculated value.

If both are equal, the route is free from packet droppers. This approach was compared with 2-hop ACK and watchdog. As this method requires an acknowledgement for each packet, it significantly improves the overhead at the same time having best delivery ratio of packets and detection ratio.

A summary of the characteristics of the surveyed schemes is presented in Table 1. The table gives the advantages and limitations of one mechanism over the other. So that an efficient method can be developed that merges the benefits of more than one mechanism to mitigate selfishness on packet forwarding. The features of each mechanism are highlighted based on the following metrics:

The overhead generated by the mechanism in terms of the new packets sent and the extra computations required carrying out the mechanism.

Is the mechanism providing any reaction technique to penalize the detected attackers?

The architecture of the mechanism: centralised, distributed or stand-alone; defined as follows:

Centralised: The core part of the mechanism is running on a unique supervisor node which monitors the whole network and the rest of the node sin the network need to report to the supervisor node for information processing.

Distributed: All the nodes run the same mechanism.

Stand-alone: All the nodes run the same mechanism however the communication between nodes is not necessary.

3. CONCLUSION

This paper addresses the various work carried out by the researchers to detect and prevent selfish behavior on packet forwarding. The major contributions are classified into incentive-based, reputation-based and other mechanism. This paper gives a glimpse of various solutions proposed to detect and isolate the selfish behavior of mobile nodes so that the network performance can be improved significantly. A comparative study of the proposed schemes gives the advantages and limitations of one scheme over the other. We concluded that most of the proposed schemes have their own limitations because of the assumption that are not valid due to the dynamic nature of the MANETs. A novel method, which can reduce the effect of selfish misbehavior and stimulates node cooperation, is the need of the hour. We hope that it is an interesting area for further explorations with more realistic assumptions and less overhead especially tailored to mitigate selfish misbehavior on packet forwarding.

Table 1. A summary of the characteristics of the Surveyed Schemes

	Characteristics			
	Architecture	**Computational Overhead**	**Communication Overhead**	**Punishment**
Nuglets [4]	Stand-alone	Low	No	Yes
L. Buttyan [5]	Stand-alone	Low	Low	Yes
Sprite [6]	Centralized	Medium	Medium	Yes
SIP [7]	Stand-alone	Low	Low	Yes
FESCIM [8]	Hybrid	Medium	Low	No
Watchdog [9]	Distributed	Low	No	No
CORE [11]	Distributed	Low	Low	Yes
CONFIDANT [12]	Distributed	Low	Low	Yes
SORI [13]	Distributed	Low	Low	Yes
Reputation-based [14]	Distributed	Low	No	Yes
Friends and Foes [15]	Distributed	Low	High	Yes
S. Buchegger [16]	Distributed	Low	No	Yes
Packet Droppers [17]	Distributed	Medium	Medium	Yes
2ACK [18]	Stand-alone	Low	Low	No
N. Jamal [19]	Distributed	Medium	Low	Yes
OMH [20]	Stand-alone	Medium	Medium	No
COFFEE [21]	Stand-alone	Medium	Medium	No
ICARUS [22]	Centralized	Low	Medium	Yes
A. Baadache [23]	Stand-alone	High	High	No

4. ACKNOWLEDGMENTS

The authors would like to thank the anonymous reviewers for their comments and suggestions.

5. REFERENCES

[1] D. Djenouri, L. Khelladi, A Survey of Security Issues in Mobile Ad Hoc Networks and Sensor Networks, IEEE Communication Surveys ant Tutorials, 7 (2005), 2-28.

[2] S. Djahel, F. Nait-Abdesselam, Z. Zhang, Mitigating Packet Dropping Problem in Mobile Ad Hoc Networks: Proposals and Challenges, IEEE Communications Surveys and Tutorials, 13 (2011), 658-672.

[3] M. Omar, Y. Challal, A. Bouabdallah, Certification-based trust models in mobile ad hoc networks: A survey and taxonomy, Journal of Network and Computer Applications 35 (2012) 268–286

[4] L. Buttyan, J. Hubaux, Nuglets: a Virtual Currency to Stimulate Cooperation in Self-Organized Mobile Ad Hoc Networks, Swiss Federal Institute of Technology, Lausanne, Switzerland, DSC/2001/001, (2001)

[5] L. Buttyan, J. Hubaux, Stimulating Cooperation in Self-Organizing Mobile Ad Hoc Networks, ACM/Kluwer Mobile Networks and Applications, 8 (2003) 579-592

[6] S. Zhong, J. Chen, Y.R. Yang, Sprite: a simple, cheat-proof, credit- based system for mobile ad-hoc networks, Twenty-Second Annual Joint Conference of the IEEE Computer and Communications, New Haven, CT, USA, (2003) 1987 - 1997.

[7] Y. Zhang, W. Lou, Y. Fang,"A Secure Incentive Protocol for Mobile Ad Hoc Networks, Wireless Networks, 13 (2007) 569-582

[8] M.M.E.A. Mahmoud, Xuemin (Sherman) Shen, FESCIM: Fair, Efficient, and Secure Cooperation Incentive Mechanism for Multihop Cellular Networks, IEEE Transactions on Mobile Computing, 11 (2012) 753 - 766

[9] S. Marti, T.J.Giuli, K. Lai, M. Baker, Mitigating Routing Misbehavior in Mobile Ad Hoc Networks, In proc. 6th annual international conference on Mobile Computing and Networking (MOBICOM '00), Boston, Massachusetts, (2000) 255-265.

[10] D.B. Johnson, D.A. Maltz, The Dynamic Source Routing Protocol for Mobile Ad Hoc Networks (Internet-Draft), Mobile Ad Hoc Network (MANET) Working Group, IETF, 2004.

[11] P. Michiardi, R. Molva, CORE: A Collaborative Reputation Mechanism to enforce node cooperation in Mobile Ad Hoc Networks, Research Report RR-02-062, 2001.

[12] S. Buchegger, Jean-Yves Le Boudec, Performance analysis of the CONFIDANT protocol, in 3rd ACM international symposium on Mobile ad hoc Networking & Computing (MobiHoc '02), (2002) 226 - 236.

[13] Q. He, D. Wu, P. Khosla, SORI: A Secure and Objective Reputation-based Incentive Scheme for Ad-hoc Networks, IEEE Wireless Communications and Networking Conference (WCNC), 2004.

[14] M. Tamer Refaei, Vivek Srivastava, Luiz DaSilva, Mohammed Eltoweissy, A Reputation-based Mechanism for Isolating Selfish Nodes in Ad Hoc Networks, International Conference on Mobile and Ubiquitous Systems: Networking and Services (MobiQuitous '05), (2005) 3-11.

[15] H Mirand, L Rodrigues, Friends and Foes: Preventing Selfishness in Open Mobile Ad Hoc Networks, International Conference on Distributed Computing Systems Workshops (ICDCSW’03), (2003) 440-445.

[16] Buchegger S and Boudee J, Self-Policing Mobile Ad Hoc Networks by Reputation Systems, IEEE Communications Magazines, 43 (2005) 101-107

[17] Djamel Djenouri and Nadjib Badache, On eliminating packet droppers in MANET: A modular solution, Ad Hoc Networks, 7 (2009) 1243-1258

[18] Kejun Liu, Jing Deng, P.K. Varshney, K. Balakrishnan, An Acknowledgment-based Approach for the Detection of Routing Misbehavior in MANETs, IEEE Transactions on Mobile Computing, 6 (2007) 536 - 550

[19] N. Jamal, Al-Karaki, A.E. Kamal, Stimulating Node Cooperation in Mobile Ad Hoc Networks, SpringerLink Wireless Personal Communications, 44 (2008) 219-239

[20] S. Chengqi, Z. Qian, OMH - Suppressing Selfish Behavior in Ad Hoc Networks with One More Hop, SpringerLink Mobile Networks and Applications, 14 (2009) 178-187

[21] S. Chengqi, Z. Qian, Protocol for Stimulating Packet Forwarding in Wireless Ad Hoc Networks, IEEE Wireless Communications, 17 (2010) 50-55

[22] D.E. Charilas et al, ICARUS: hybrId inCentive mechAnism for coopeRation StimUlation in ad hoc networkS, Ad hoc Networks,

[23] A. Baadache, A. Belmehdi, Fighting against packet dropping misbehavior in multi-hop wireless ad hoc networks, Journal of Network and Computer Applications 35 (2012) 1130–1139

AUTHORS BIOGRAPHY

Prof. P. Mani received her B.Sc., and MCA degrees from Bharathiar University, Coimbatore. She is a part-time research scholar at Anna University, Chennai and working as a Head and Assistant Professor in Department of MCA at M. Kumarasamy College of Engineering, Karur. Her research interest includes Wireless Ad Hoc Networks especially on routing protocols and security.

Dr. P. Kamalakkannan received his B.Sc., MCA., degrees from Bharathiar University, Coimbatore and Ph.D. from Periyar University, Salem. Since 1991, he has been serving to the student community as Professor, Head and Director. Currently, he is an Assistant Professor at PG and Research Department of Computer Science in Government Arts College (Autonomous), Salem, affiliated to Periyar University. He is guiding 12 research scholars. His research interests include Computer Networks, Wireless Communications, Image Processing, Parallel and Distributed Computing. He is have more than 50 International and National research publications in various Journals and Conferences. He is a journal reviewer of IJOPCM, IJCSA and also reviewer of various International Conferences.