Crossroads
The ACM Student Magazine

Overcoming Misbehavior in Mobile Ad Hoc Networks: An Overview

by ***George Athanasiou***, ***Leandros Tassiulas***, ***Gregory S. Yovanof***

Introduction

In the recent years, wireless networks have experienced an enormous growth which has given rise to new research challenges. Ad hoc networks are composed of autonomous nodes that are independent of any fixed infrastructure. Mobile ad hoc networks have a fully decentralized topology and they are dynamically changing. Besides these challenges, the wireless transmission medium introduces limitations in communication. For these reasons, providing security guarantees is particularly difficult. In a mobile ad hoc network every node acts as a router for its neighbors. The routing protocols that have been proposed assume that the nodes will fully participate. Unfortunately, node misbehavior is a common phenomenon. Misbehavior is due to selfish or malicious reasons. Another reason, which is rarer, is a faulty link due to the wireless medium. Misbehavior can take place at all layers. At the Physical layer a misbehaving node can increase its transmitting power, adversely affecting the network performance. At the MAC (Medium Access Control) layer a node may choose to avoid waiting for its turn to access the medium, taking an unfair advantage of the shared medium. The basic threat at the Network layer is the non-cooperative behavior as far as packet forwarding is concerned. The proper execution of a routing protocol demands that the intermediate nodes in a path forward the packets correctly to the intended receivers. Misbehaving nodes do not forward these packets. A routing protocol for MANETs should give incentives for cooperative action or at least it should be able to detect misbehaving nodes and correct them.

At the Transport layer no misbehavior problems have been identified for mobile ad hoc networks. At this layer there is a research action that aims to improve the performance of TCP over wireless networks. At the Application layer there is a huge effort of developing applications that can perform well over mobile ad hoc networks. The misbehavior problem is not yet clearly addressed in this area. Only a few intrusion detection techniques exist that operate at this layer which are based on trace analysis of historical data. We only briefly touch upon this issue, as intrusion detection is beyond the scope of this paper. Our objective in this

paper is to present a classification of misbehavior techniques according to the layer to which they are applicable. However, some of them have cross-layer features.

We organize this paper as follows. In next two sections, we discuss further the misbehavior problem at the MAC and Network layer respectively and we describe some proposals that address these problems. A proposal for misbehavior detection in infrastructure wireless networks follows. Finally, we conclude with the presentation of future directions.

MAC Layer Misbehavior

One of the most widely used RF technologies in mobile ad hoc networks is the IEEE 802.11 (Wi-Fi) protocol [**12**]. The MAC of this scheme is based on the CSMA/CA mechanism for sharing the wireless medium. A special mode of the 802.11 MAC is the DCF (Distributed Coordination Function), which is a distributed mechanism that permits the operation of Wi-Fi in an ad hoc manner. With this mechanism each node has a CW (Contention Window) variable. When there is a collision, a node has to wait before retransmission for a random period of time between 0 and CW (backoff value). While the channel is idle, the backoff value is decremented by one at each time slot and when the channel is busy there is no change in the backoff value. The node has the right to transmit when the backoff value is equal to 0. After the transmission there is an adjustment to the CW. If the transmission is successful, then the CW will be reset; but in the case of non successful transmission the CW doubles up.

A misbehaving node can gain more bandwidth when selecting a smaller backoff value than the DCF specifies or when, after a failed transmission, the node does not double up the CW variable. But such a misuse of the backoff mechanism has a detrimental effect on the other nodes' throughput, restricting their fair access to the medium. An example will be described during the discussion of a proposal for the detection of MAC layer misbehaviors.

MAC Layer Misbehavior Detection and Response Proposals

In this section we introduce some representative systems that have been proposed recently and which aim at detecting certain kinds of misbehavior at the MAC layer. Moreover, when a misbehavior tactic is detected, these systems use different techniques to respond in an unsupervised fashion to reinstate the proper execution of the MAC mechanism and further to enforce cooperation.

Cardenas et al. [**7**] study the effect of MAC layer misbehavior in ad hoc wireless networks. They argue that the CSMA/CA scheme, that is used in IEEE 802.11, is not resilient to selfish behavior and denial of service (DoS) attacks. In their work, they have investigated the selfish behavior achieved by manipulating the backoff mechanism of IEEE 802.11 MAC protocol [**12**] and they have proposed an extension to the 802.11 CSMA/CA protocol to remedy this. They introduce a distributed random backoff value selection. Both the receiver and the sender know

this random backoff value. In that way, the receiver can monitor the behavior of the sender and can report selfish behavior to the reputation management system. They use a reputation management system similar to CONFIDANT [4], another misbehavior detection scheme that will be described later. **Figure 1** shows a scenario where nodes M and D collude with the intent to interfere in the communication path of nodes B and C.

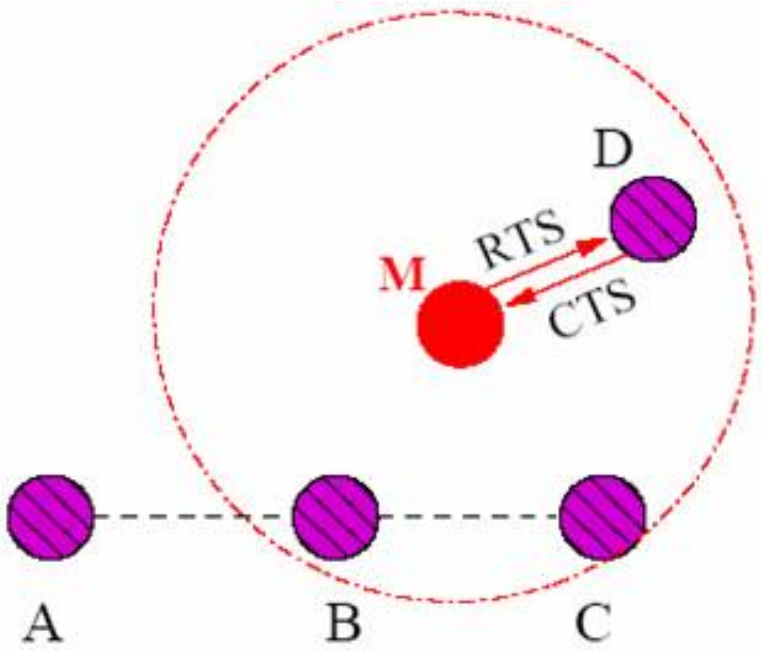

Figure 1: Nodes M and D collude and interfere in the communication path of nodes B and C [7].

Figure 2 shows how nodes M and D collude and select a very small backoff, thereby denying access to node A by causing CTS timeouts. At the end of this paper several algorithms are introduced that manage the detection of backoff manipulation by a pair of colluding nodes. These algorithms are designed for mobile ad hoc networks but they can be applied to infrastructure wireless networks (Wireless Local Area Networks) as well.

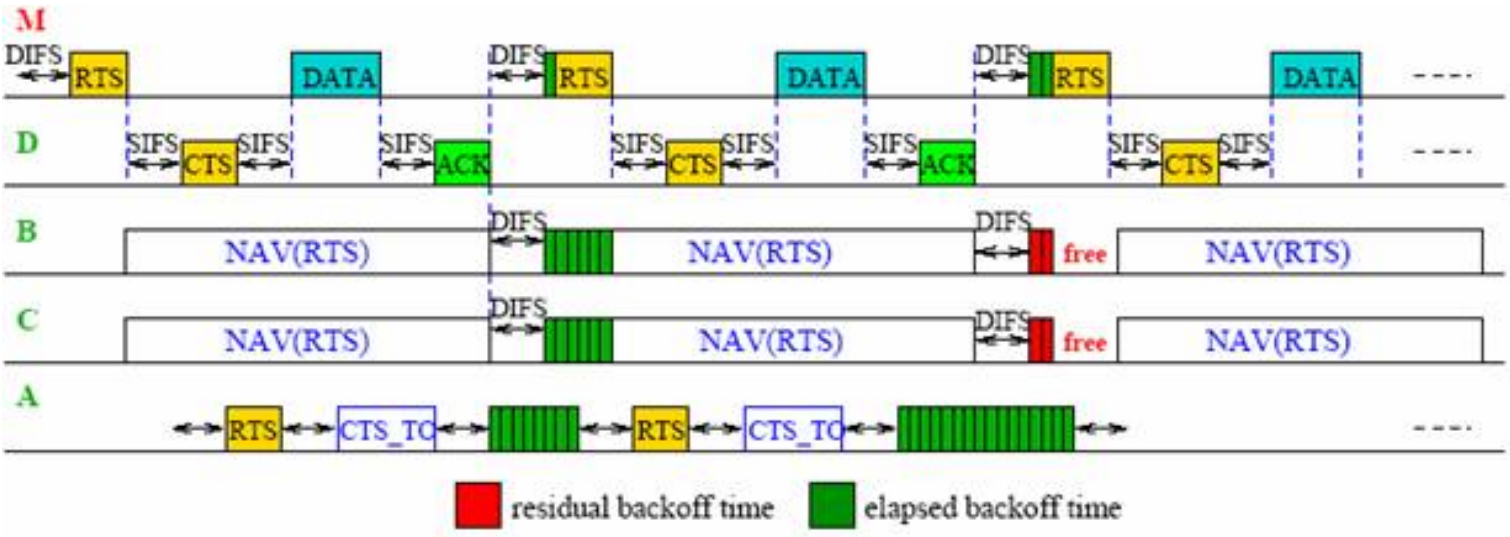

Figure 2: Nodes M and D collude and select a very small backoff, thereby denying access to node A by causing CTS timeouts [7].

Kyasanur & N. Vaidya [11] also focus on the misbehavior problem that may arise in 802.11 ad hoc networks. They briefly describe the MAC operation, point out its inability to cope with misbehavior, and propose a modification to the IEEE 802.11 protocol to simplify detection of selfish hosts. Moreover, they suggest an automatic system response when misbehavior is detected. In their approach the backoff value is determined by the receiver and can be used by the sender. The main problem here is that the receiver must be a trusted host. In that way the receiver can detect any misbehavior by increasing the backoff value during the next transmission. The proposed scheme has three steps:

1. At the end of the transmission, the receiver searches whether the sender deviated from the protocol.
2. If the receiver has identified a deviation, then it corrects the sender. The correction is based on the type of deviation that takes place.
3. If the deviation of a sender over multiple transmissions exceeds a threshold, then the receiver claims that the sender is indeed misbehaving.

The simulation results indicate that the proposed scheme is successful in handling MAC layer misbehavior. **Figure 3** shows the throughput comparison between IEEE 802.11 and the proposed scheme.

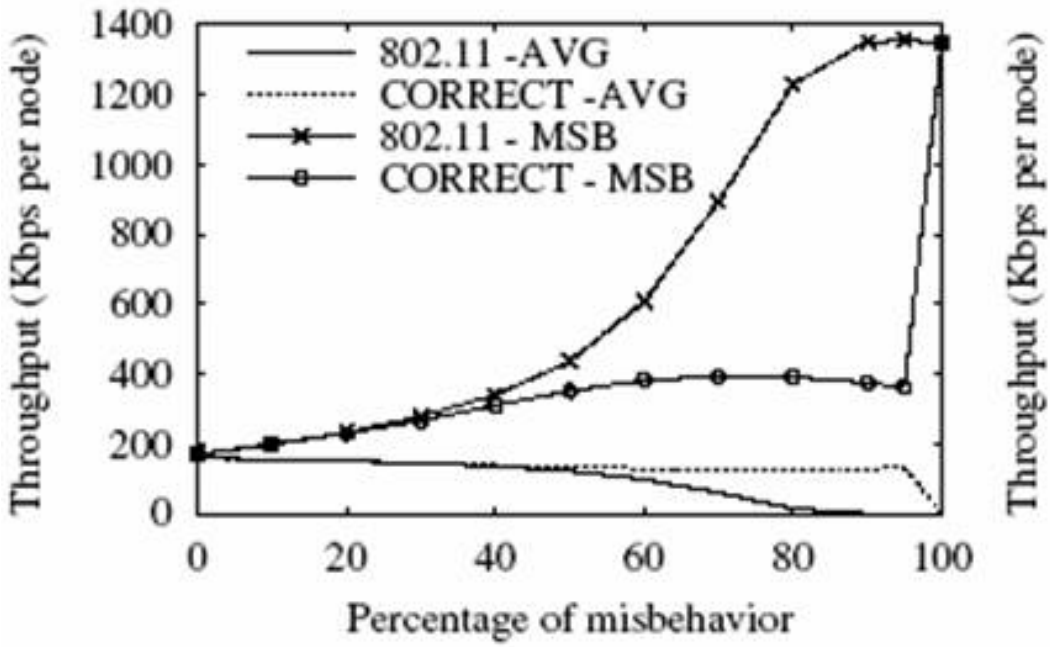

Figure 3: Throughput comparison between IEEE 802.11 and the proposed scheme [11].

Network Layer Misbehavior

Routing protocols (e.g., DSR, Dynamic Source Routing) [**10**] base their efficiency in the cooperation between the mobile nodes. But what is node cooperation at the Network layer? First of all a node that is part of a mobile ad hoc network must participate in the routing process. During the path discovery phase, a well-behaved node who receives route requests has to respond with valid information. In the data transmission phase, nodes must forward packets that reach them to the correct destination.

Misbehavior at the Network layer is the aberration of the above "normal" behavior. It is interesting to investigate the reasons that drive the nodes to misbehave. Firstly, a node may possibly have a fault which affects the node's behavior. In addition, it can gain significant advantages by misbehaving. A node may choose not to forward a packet in order to save power. The result of such misbehavior is reduction of the overall throughput and packet loss increment. The availability of the network, as far as routing is concerned, is very low. The major research effort that focuses on the misbehavior problem is taking place at the Network layer. The main proposals are described below.

Network Layer Misbehavior Detection and Reputation-based Proposals

In this section we describe systems that have been proposed recently, whose objective is to detect misbehavior at the Network layer.

The first proposal for detecting routing misbehavior in mobile ad hoc networks was by Sergio Marti et al [**13**]. This system manages to identify misbehaving hosts, and exclude them from taking part of general network operations, such as routing. In their approach, a *watchdog* is used to identify misbehaving nodes and a *pathrater* helps routing protocols to avoid these nodes. More specifically, the *watchdog* detects the denial of packet forwarding by a node and flags it so that it will be avoided by the routing protocol. The authors focus on the performance hit that occurs when misbehaving nodes are part of an ad hoc wireless network. In simulations we can see that as a result of applying the watchdog mechanism, the throughput is increased by 17% in a network with moderate mobility. The ratio of overhead transmission to data transmissions from standard routing protocols is increased from 9% to 17%. In case of extreme node mobility the throughput is increased by 27%, while increasing the percentage of overhead transmissions from 12% to 24%. **Figure 4** shows the overall network throughput as a function of the fraction of misbehaving nodes in the mobile ad hoc network.

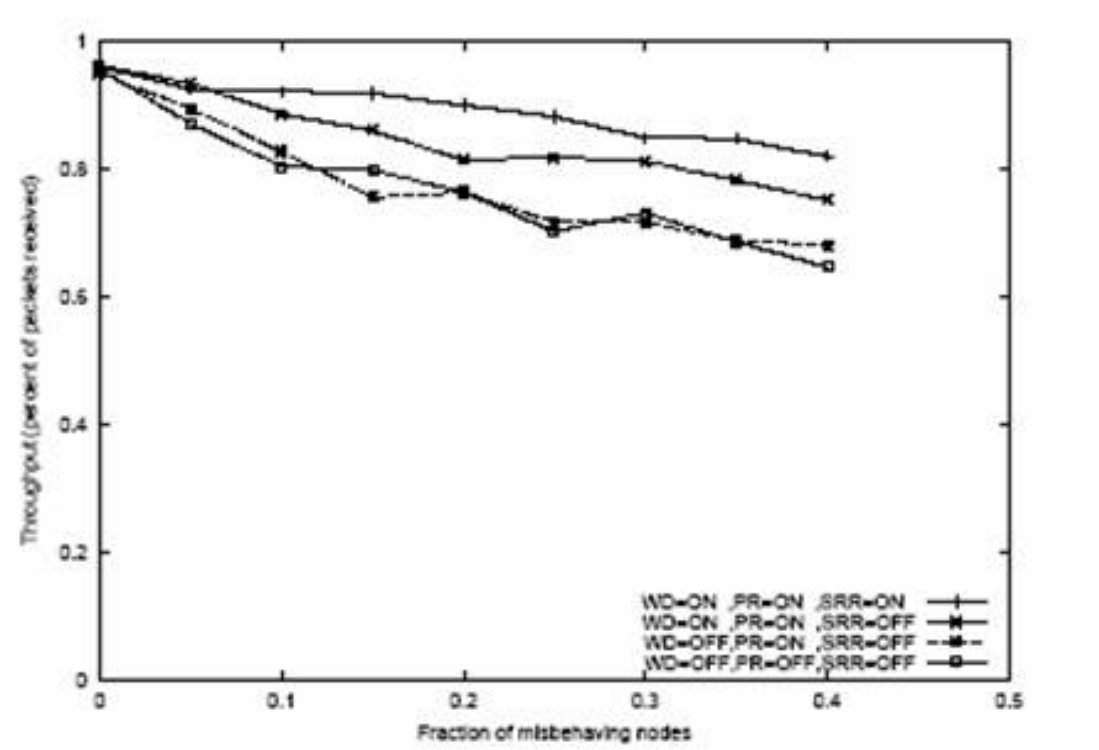

Figure 4: Overall network throughput as a function of the fraction of misbehaving nodes in the network [**13**].

The OCEAN [**2**] is using direct, first-hand observations of other nodes' behavior for detecting and mitigating misleading routing behavior in ad hoc networks. Directly observed positive behavior increases the rating, while directly observed negative behavior decreases it by an amount larger than that used for positive increments. The mechanism proposes a rating threshold. If the rating of a node is below the threshold, then the node is added to a faulty list. All route requests contain this faulty list. Each node that receives a route request avoids routing to the nodes that are part of the faulty list. **Figure 5** shows the average throughput of misleading nodes with varying Faulty Timeout and Faulty Threshold parameters.

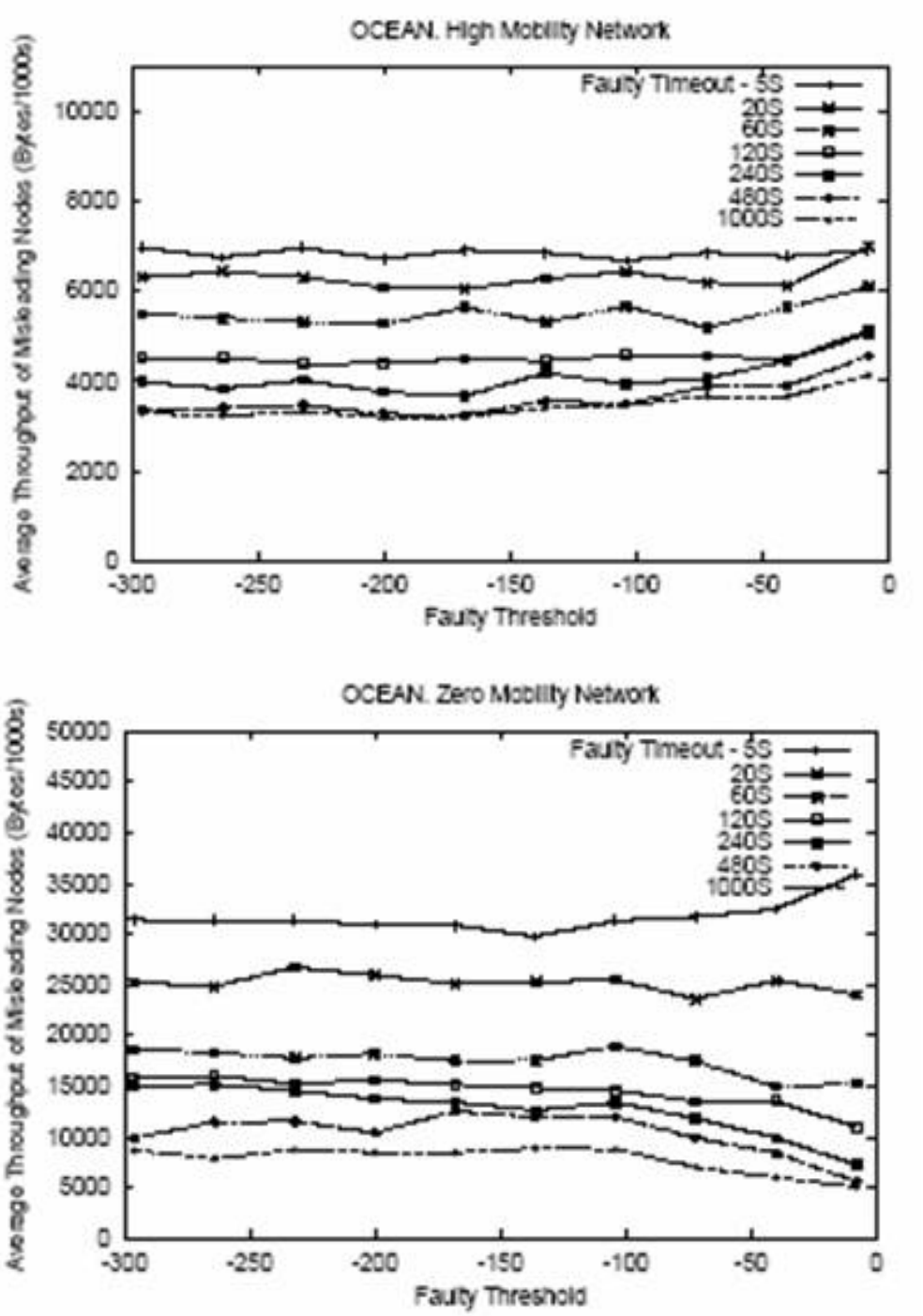

Figure 5: Average Throughput of Misleading Nodes with varying Faulty Timeout and Faulty Threshold parameters (high mobility network & zero mobility network) [**2**].

Pietro Michiardi and Refik Molva proposed the CORE generic mechanism [**15**], which is based on a reputation metric that can be used to enforce the cooperation and prevent selfish behavior. The result of this selfish behavior is the passive denial of service. Each node has a record of the reputation of the other nodes. The reputation of each node is calculated with the use of various types of information. This generic mechanism is implemented as an extension of existing protocols. This approach makes use of a component similar to the *watchdog* [**13**] scheme that we described above. The functionality of this component is based on reputation. The CORE mechanism can be integrated with several network and application layer functions

whereas the *watchdog & pathrater* scheme is specifically designed for routing.

Sonja Buchegger and Jean-Yves Le Boudec, [**3**, **4**] focus on the cooperation, robustness, and fairness that must be established in a "healthy" mobile ad hoc network. Their protocol, dubbed CONFIDANT, is based on the monitoring of node behavior. The monitoring results are an important piece of information that the system uses in order to evaluate the reputation of corresponding nodes and punish selfish nodes. An important part of this protocol is that nodes learn not only from their own experience, but also from observing the neighborhood and from the experience of their "friends". The main problem of the CONFIDANT protocol is that it punishes the nodes if they do not forward packets regardless of how they have previously contributed to the network. Thus, the nodes that are part of the mobile ad hoc network, and especially the nodes that are placed in the center of the network, in their attempt to avoid being designated as selfish, forward each packet that they receive. The impact of this behavior is that the network efficiency drops. The authors have chosen the Dynamic Source Routing (DSR) [**10**], as the base protocol for the simulation of the CONFIDANT protocol. During their simulation they prove that the CONFIDANT protocol performs well even with a fraction of malicious nodes as high as 60%. **Figure 6** shows the mean client and server throughput in a network of 50 nodes with one third malicious, over 20 simulation runs.

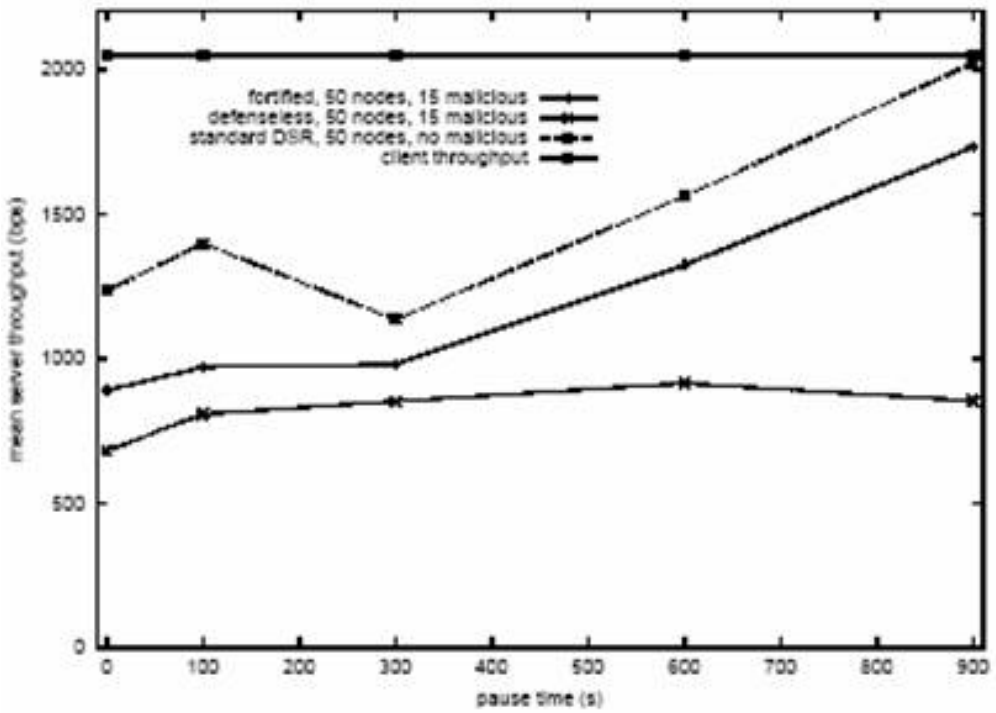

Figure 6: Mean client and server throughput in a network of 50 nodes with varying mobility and with one third malicious. The results have been averaged over 20 simulation runs [**3**, **4**].

The protocol proposed in [**16**], uses the concept of "justified selfishness" which makes the system fairer. The scheme by Miranda et al. uses a period broadcasting mechanism. Each node

in the network periodically sends its "opinion" about neighbors. Besides this, a node can refuse any of the route requests that it receives or drop received packets. The nodes publicize reasons for their behavior. The community evaluates whether the proportion of refused hosts reaches an unacceptable level of selfishness. Unfortunately, the overhead of communications among the nodes becomes huge, compared to the size of the packets.

Krishna Paul and Dirk Westhoff in [**17**], have attempted to detect a large range of attacks on the Dynamic Source Routing (DSR) protocol [**10**]. Their mechanism is an extension of the DSR. The decision of how to treat nodes in the future is based on accusations of others. For the number of accusations pointing to a single attack, the approximate knowledge of the topology and context-aware inferences are utilized to enable a node to rate an accused node without doubt. But nodes must reach a consensus as far as accusations are concerned, otherwise when a single node makes an accusation it is accused of misbehavior.

Yi-an et al. focus their research on techniques for automatically constructing anomaly detection models that are capable of detecting new or unknown attacks [**9**]. In this proposal the anomaly detection problem is converted into a set of classification sub-problems. Correlations between features play an important role in this procedure. They use new data mining techniques for capturing the inter-feature correlation patterns.

The proposal in [**19**] is a distributed intrusion detection system where there is an agent at each node, that communicates with the agents of the other nodes. This approach is based on statistical anomaly-detection and integration of intrusion-detection information from several networking layers. The trace analysis and anomaly detection is done locally at each node as well as through cooperation with all nodes in the network. This approach uses Application/ Session layer functions (trace analysis and historical statistics analysis). **Figure 7** shows the architecture of an Intrusion Detection agent (ID agent).

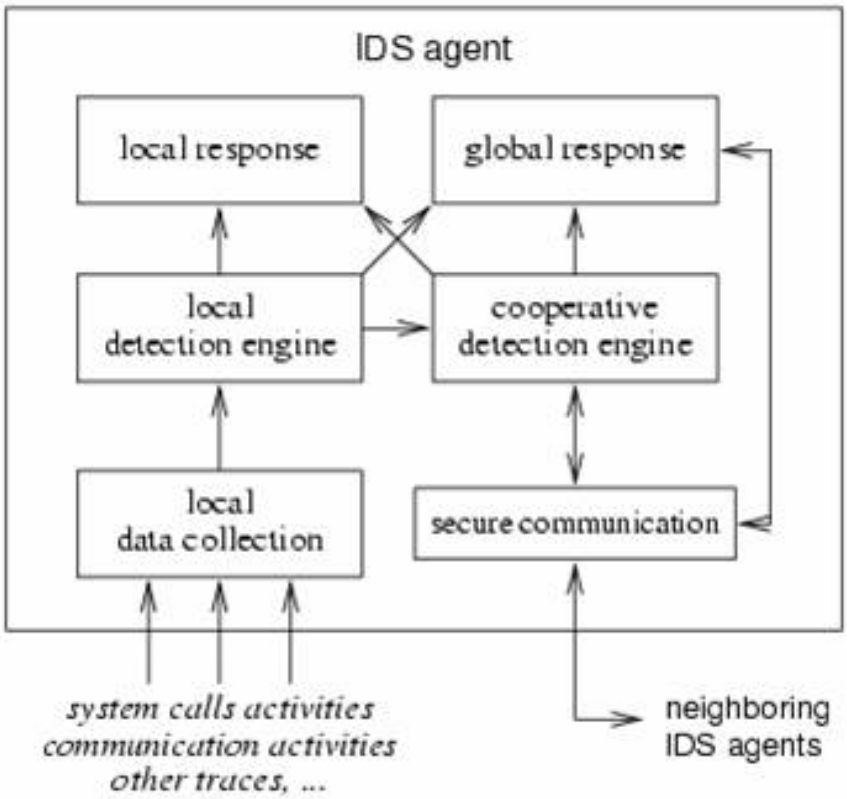

Figure 7: Architecture of an Intrusion Detection Agent [19].

Economic Incentive Proposals

In this section we present incentive-based protocols that address different misbehavior problems in mobile ad hoc networks and try to cope with them by attempting to reinforce cooperation. Most of these systems use economic incentives. In networks with distributed control logic, the individual nodes lack a strong incentive to forward packets for the benefit of the other nodes.

In [6] the authors consider where each node is its own authority. In this self-organizing mobile ad hoc network, a mechanism must exist to stimulate cooperation between nodes. This proposal uses a credit counter module in each node. The counter decreases when the node sends a packet and increases when the node forwards a packet (the counter must be positive). Besides this counter mechanism, a security mechanism is implemented at each node. This security mechanism is responsible for the protection of packet header (cryptography) and the secure maintenance of the nodes' counter value.

Levente Buttyan and Jean-Pierre Hubaux [5] describe the service availability problem that exists in mobile ad hoc WANs. In their approach, they introduce the concept of "money" and "service charges." More specifically, they use virtual currency that they call nuglets. As in real life, nodes try to earn as much nuglets as possible. They use two models for node "payment" of packet forwarding: the Packet Purse Model and the Packet Trade Model. In the Packet Purse Model the sender of a packet is responsible for the node "payment". Here, each node is

"paid"with one nuglet to forward a packet. The main problem is that the system must calculate the amount of the nuglets that must be used for a packet transmission. In the case of nuglet absence, the packet must be dropped, and in the case of nuglet redundancy, the nuglets that have not been used are lost. The authors suggest that this problem can be solved if the system lets users buy nuglets during a packet transmission. In the Packet Trade Model, the receiver pays for the packet transmission. Each intermediate node "buys" a packet for some nuglets, and "sells" it to the next one for more nuglets. Therefore a node increases its nuglet amount during packet forwarding. The main problem here is the efficiency of the network. Nodes try to find a neighbor that "pays" the highest for its packet. Nodes don't take the shortest routing path for the packet transmission. **Figure 8** illustrates the Packet Purse Model and the Packet Trade Model.

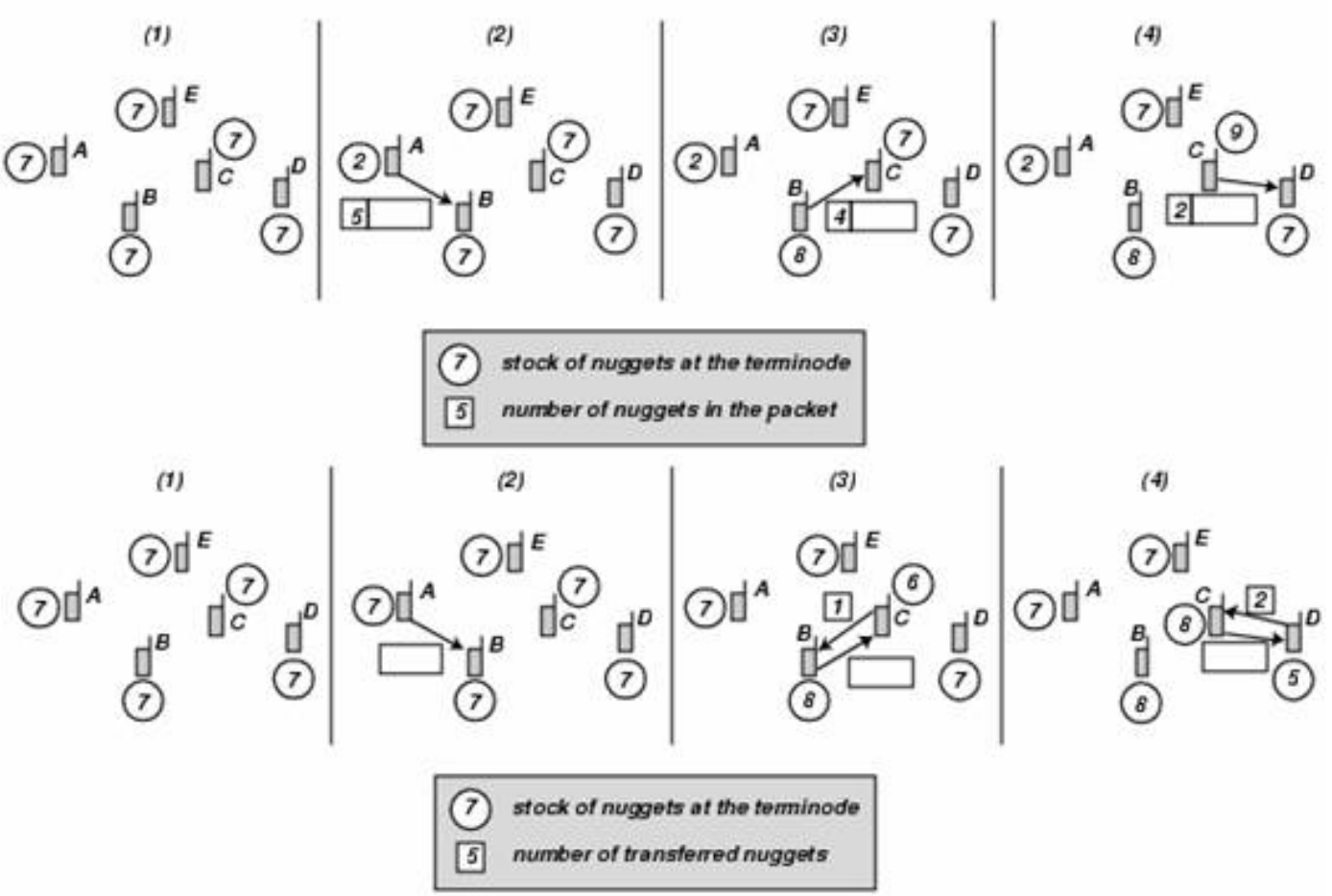

Figure 8: Packet Purse Model and Packet Trade Model [5].

The SPRITE system proposed in [20] uses a credit-based mechanism which provides incentives for mobile nodes to cooperate. An important part in this scheme is the Credit Clearance Service (CCS). A summary of the basic system's functionality is as follows. Each node that receives a message keeps a receipt of the message. This receipt contains a hash of the received message. During the next step, the node uploads the receipt to the CCS and confirms that the message was received or forwarded. The CCS charges the origin node who is the source of the message. This charge is based on the number of the receipts that the sent

message contains and the number of the intermediate nodes that the message passed to reach its destination. If a node has forwarded a message and its receipt has not been uploaded to the CCS, then the intermediate node will not be involved in calculating the charges. Finally, when the charging is finished, the origin node must "pay" the intermediate nodes. The availability of the trusted CCS is a crucial point. Thus, the authors have introduced secure routing techniques and a public key infrastructure to ensure availability. **Figure 9** shows the architecture of SPRITE.

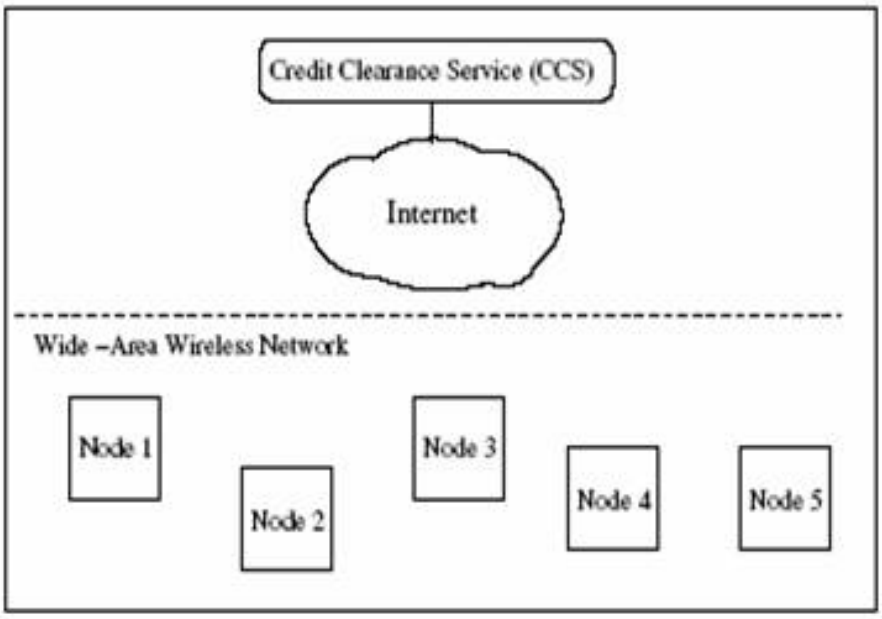

Figure 9: The architecture of SPRITE [**20**].

Raghavan and Snoeren have introduced the priority forwarding case [**18**]. The authors argue that the main aspect in a "healthy" ad hoc network is the cooperation among the nodes to forward packets. In their proposal, the pricing mechanism allows the nodes to arbitrarily set the cost of priority forwarding of a packet (k node has a cost ck). During payment the system pays each node for forwarding a packet . This payment amount must be bigger than or equal to the cost ck set by the node. When a node receives a packet it can drop the packet or it can forward the packet to another node.

Fratkin et al. [**8**] employ a virtual economy scheme, called Ad Hoc Participation Economy (APE). This scheme tries to adjust the natural equilibrium in ad hoc networks and presents enough incentives to ensure that their routing behavior will be normal. The nodes receive "money" in order to forward some other node's packets. As with real economies this virtual economy monitors the payment process with "banking nodes". These nodes assure payment consolidation and its integrity. This central service approach is different from other incentive-based schemes. In APE, when a node wants to communicate with another, it initiates a route discovery protocol. This protocol must calculate the exact amount of "money" that the source node needs to "pay" for a packet transmission. **Figure 10** shows an example where node A

wants to send a message to node B. The routing discovery protocol chooses the cheapest route (through C).

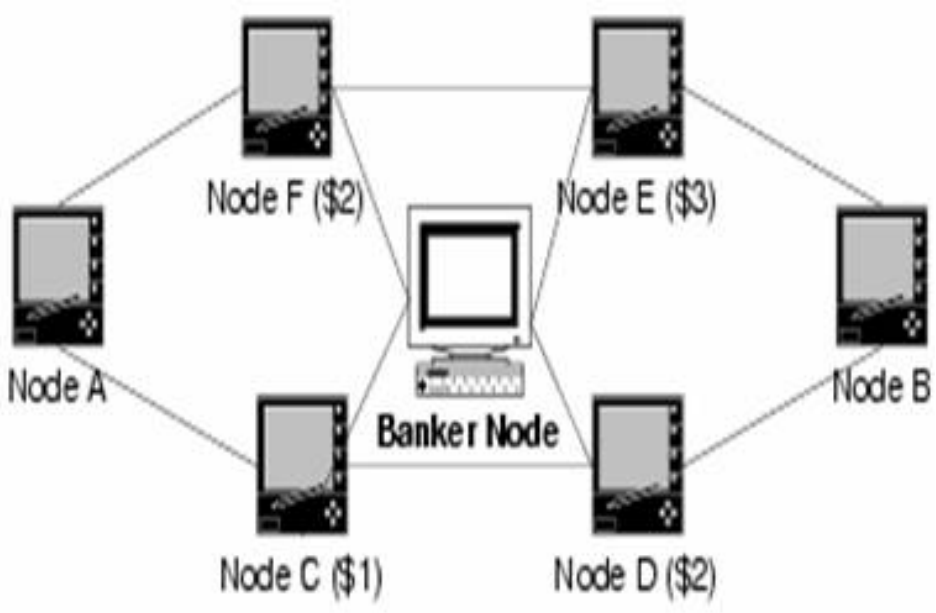

Figure 10: Routing example [8].

Anderegg and Eidenbenz propose a protocol which manages to cope with greedy or selfish agents in a mobile ad hoc network [1]. The goal of this protocol is to encourage the intermediate nodes to reveal the cost of packet forwarding. Thus, a cost-efficiency route can be chosen. Ad hoc-VCG consists of two phases: Route Discovery and Data Transmission. During the Routing Discovery phase a cost computation for a packet transmission exists. The result of this computation is a minimum cost route from the packet's source to its destination. **Figure 11** depicts an example of the cost calculation process. The "cheapest" route is S, v2, v3, D. The data transmission phase uses this route for the packet transmission. In the latter phase, the intermediate nodes are "paid" for their packet forwarding services.

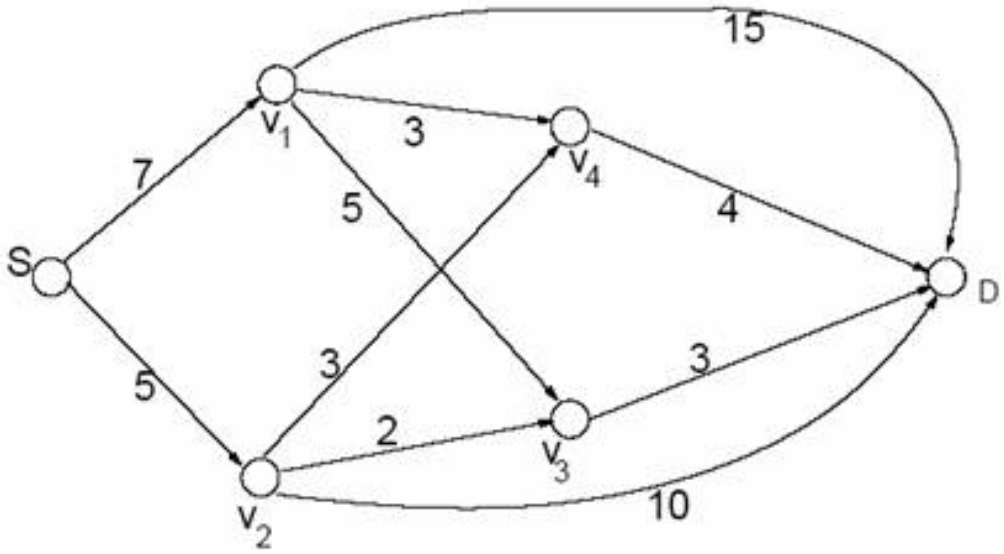

Figure 11: Example of the calculation of the cost in Packet Forwarding [1].

Infrastructure Wireless Networks

Infrastructure wireless networks are not as vulnerable to misbehavior because they have a more centralized architecture than mobile ad hoc networks. Pervasive deployment of hotspots and public internet access, however, generates a host of new problems.

Maxim Raya et al. [**14**] introduce the main misbehavior problems that are likely to happen in the deployment of IEEE 802.11. These main problems occur at hotspots that provide public wireless internet access [**12**]. Their system DOMINO, can detect MAC layer greedy behavior. DOMINO is software installed at the Access Points and does not affect the authentication process. In most cases individual users have to pay for hotspot internet access. This can motivate them to increase their share of the medium and thus gain network bandwidth. Unfortunately, this motivation can adversely affect the allocation of bandwidth to other users. DOMINO copes with this problem by comparing an average value of the backoff to a given threshold. This procedure uses only statistical data analysis and is integrated in the AP functionality.

Conclusions And Future Directions

A node's misbehavior can have severe impact in overall network performance. This paper has presented an overview of state-of-the-art systems that try to detect and correct a node's selfish or malicious misbehavior by giving incentives to the nodes so that they will cooperate. Unfortunately, the misbehavior problem has not yet been addressed adequately.

Misbehavior at any given layer cannot always be detected. The security management in mobile ad hoc networks is by nature a cross-layer issue. Therefore, security management must detect across layers and respond to misbehavior problems as well. This is a very difficult task because in a cross-layer perspective, different protocols must exist at each layer and communicate with each other. In addition, cross-layering gives rise to new threats. The different layers in the network stack communicate regularly with each other and misbehavior can expand. In general, the study and investigation of systems that can holistically address misbehavior tactics and span different layers of the network stack is a field that will attract much research in the near future.

References

19-1

Anderegg, L., and Eidenbenz, S. (2003). Ad hoc-VCG:A Truthful and Cost-Efficient Routing Protocol for Mobile Ad hoc Networks With Selfish Agents. In *Proceedings of ACM/ IEEE International Conference on Mobile Computing and Networking (Mobicom'03)*, San Diego, CA.

6-2

Bansal, S., and Baker, M. (2003). Observation-based cooperation enforcement in ad hoc networks. *Technical Report*.

9-3

Buchegger, S., and Le Boudec, J. Y. (2002). Nodes bearing grudges: Towards routing security, fairness, and robustness in mobile ad hoc networks," In *Proceedings of 10th Euromicro PDP (Parallel, Distributed and Network-based Processing)*", Gran Canaria, 403-410.

8-4

Buchegger, S., and Le Boudec, J.-Y. (2003). Performance analysis of the confidant protocol. In *Proceedings of the 3rd ACM International Symposium on Mobile Ad Hoc Networking & Computing*, 226-236.

15-5

Buttyan, L., and Hubaux, J.-P. (2000). Enforcing service availability in mobile ad-hoc wans. In *Proceedings of IEEE/ACM Workshop on Mobile Ad Hoc Networking and Computing (MobiHOC)*, Boston, MA.

14-6

Buttyan, L., and Hubaux, J.-P. (2001). Stimulating cooperation in self-organizing mobile ad hoc networks. Technical Report DSC/2001/046, EPFLDI-ICA.

2-7

Cardenas, A. A., Radosavac, S., and Baras, J. S. (2004). Detection and Prevention of MAC Layer Misbehavior for Ad Hoc Networks. *Technical Report*.

18-8

Fratkin, E., Vijayaraghavan, V., Liu, Y., Gutierrez, D., Li, T.M., and Baker, M. Participation Incentives for Ad Hoc Networks, <**http://www.stanford.edu/yl314/ape/paper.ps**>.

12-9

Huang, Y., Fan, W, Lee, W., and Yu, P. S. (2003). Cross-feature analysis for detecting ad hoc routing anomalies. In *Proceedings of the 23rd International Conference on Distributed Computing Systems (ICDCS 2003)*.

4-10

Johnson, D. B., and Maltz, D. A. (2003). The dynamic source routing protocol for mobile ad hoc networks. Internet Draft, Mobile Ad Hoc Network (MANET) Working Group, IETF, Version 9.

3-11

Kyasanur, P., and Vaidya, N. (2003). Detection and handling of mac layer misbehavior in wireless networks. In *Proceedings of the International Conference on Dependable Systems and Networks*.

1-12

L. M. S. C. of the IEEE Computer Society. (1999). Wireless LAN medium access control (MAC) and physical layer (phy) specifications. *IEEE Standard 802.11*, 1999 Edition.

5-13

Marti, S., Giuli, T. J., Lai, K., and Baker, M. (2000). Mitigating routing misbehavior in

mobile ad hoc networks. In *Proceedings of MOBICOM 2000*, 255-265.

20-14

Maxim Raya, J.-P. H., and Aad, I. (2004). Domino: A system to detect greedy behavior in ieee 802.11 hotspots. In *Proceedings of the 2nd International Conference on Mobile Systems, Applications and Services (MobiSys2004)*, Boston, MA.

7-15

Michiardi, P., and Molva, R. (2002). CORE: A collaborative reputation mechanism to enforce node cooperation in mobile ad hoc networks. In *Proceedings of the* 6th *IFIP Conference on Security Communications, and Multimedia (CMS 2002)*, Portoroz, Slovenia.

10-16

Miranda, H. and Rodrigues, L. (2003). Preventing selfishness in open mobile ad hoc networks. In *Proceedings of the International Workshop on Mobile Distributed Computing (MDC)*, Providence, RI , 440-445.

11-17

Paul, K, and Westhoff, D. (2002). Context aware inferencing to rate a selfish node in dsr based ad-hoc networks. In *Proceedings of the IEEE Globecom Conference*, Taipeh, Taiwan.

17-18

Raghavan, B., and Snoeren, A. C. (2003). Priority forwarding in ad hoc networks with self-interested parties. *Workshop on Economics of Peer-to-Peer Systems*, Berkeley, CA.

13-19

Zhang, Y., and Lee, W. (2000). Intrusion detection in wireless ad-hoc networks. In *Proceedings of MOBICOM 2000*, 275-283.

16-20

Zhong, S., Yang, Y., and Chen, J. (2003). Sprite: A simple, cheat-proof, credit-based system for mobile ad hoc networks. *Proceedings of Infocom*.

Biographies

George Athanasiou (**gathanas@inf.uth.gr**) is a 5th year B.Sc. student in the Department of Computer and Communications Engineering at the University of Thessaly. His research interests include wireless and mobile networking, security and quality of service (QoS) in mobile ad hoc networks, and distributed multimedia content delivery networks. He is currently working towards his thesis in the area of misbehavior in mobile ad hoc networks.

Leandros Tassiulas (**leandros@uth.gr**) is a Professor in the Department of Computer and Communications Engineering at the University of Thessaly, Greece. He received his M.S. and Ph.D. from the University of Maryland and his Diploma from the University of Thessaloniki, Greece in 1991 and 1987, respectively. His current research interests include wireless and

mobile communications, scheduling, and congestion control techniques in communication networks and security.

Gregory S. Yovanof (**gyov@ait.edu.gr**) is an Associate Professor and the Head of the Broadband Wireless and Sensor Networks Group at the Athens Information Technology (AIT). Prior to joining AIT, he had a long career in the hi-tech industry working on the production of broadband communication systems. His current research interests include multimedia communications and security in mobile ad hoc networks. He holds a Ph.D. in Communications from the University of Southern California.