FINDING OF SELFISH NODES AND IRRATIONAL NODES IN MULTIHOP CELLULAR NETWORK USING CRC AND HASH CHAIN MECHANISM

M.Sivasankari

VishnThulasidharan

ABSTRACT:

When we use multihop cellular network to transmit the data, the main problem is faulty nodes ands and selfish nodes.We can avoid the faulty nodes by using appropriate firewalls at the sender side and receiver side. The selfish nodes are avoid by charging the source and destination nodes when both of them benefit from the communication and it can secure the payment, charge the source and destination nodes almost computationally free, and significantly reduce the number of generated and submitted checks. In this way, each intermediate node earns some credits and the destination node pays the total packet relaying cost. To implement this charging policy efficiently, hashing operations are used in the ACK packets to reduce the number of public-key-cryptography operations. Moreover, reducing the overhead of the payment checks is essential for the efficient implementation of the incentive mechanism due to the large number of payment transactions.

KEYWORDS: *Mobile –adhoc networks, Check Submission Scheme, Check Clearances Phase, Cyclic Redundancy Check, Incentive and reputation based mechanism*

Introduction

Mobile computing is human–computer interaction by which a computer is expected to be transported during normal usage. Mobile computing involves mobile communication, mobile hardware, and mobile software. Communication issues include ad-hoc and infrastructure networks as well as communication properties, protocols, data formats and concrete technologies. Hardware includes mobile devices or device components. Mobile software deals with the characteristics and requirements of mobile applications Mobile computing is "taking a computer and all necessary files and software out into the field." "Mobile computing: being able to use a computing device even when being mobile and therefore changing location. Portability is one aspect of mobile computing." "Mobile computing is the ability to use computing capability without a pre-defined location and/or connection to a network to publish and/or subscribe to information " . This paper proposes FESCIM, a Fair, Efficient, and Secure Cooperation Incentive Mechanism, to stimulate the node cooperation in MCN. In order to efficiently and securely charge the source and destination nodes, the lightweight hashing operations are used in the ACK packets to reduce the number of public-key-cryptography operations. The destination node generates a hash chain and signs its root, and acknowledges message reception by releasing a hash value from the hash chain. In this way, the destination node generates a signature per group of messages instead of generating a signature per message. Furthermore, instead of generating a check per message or generating a nodal check for each intermediate node, a small-size check containing the payment data for all the intermediate nodes is generated per route. In addition, trusting one node to submit the check is not secure because this node may collude with the source and destination nodes to not submit the check. Instead of submitting the checks by all the intermediate nodes to thwart collusion attack, a Probabilistic Check-Submission scheme is proposed to reduce the number of submitted checks and protect against collusion attack. . As long as all nodes adhere to this and cooperate, the MANET should work without problems. One of the most important issues in designing MANET protocols is how to deal with nodes that do not cooperate. Depending on their (or their user's) motivation I will categorize these nodes into three groups:

• Malevolent nodes – Nodes that want to compromise the security of the MANET or of other nodes. Their actions are directed on some desired effect, but they are generally not rational because they do not strive for their own benefit maximization.

• Selfish nodes – Nodes that do not forward other's packets, thus maximizing their benefit at the expense of all others. They are assumed to always behave rationally, so they cheat only if it gives them an advantage.

• Erroneous nodes – These are nodes with failing hardware or incorrect software. They do not intentionally misbehave but if they impair the working of the net, then they have to be treated just as malevolent or selfish nodes.

EXISTING FEATURES & RELATED WORKS:

1. we address the problem of service availability in mobile ad-hoc WANs. We present a secure mechanism to stimulate end users to keep their devices turned on, to refrain from overloading the network, and to thwart tampering aimed at converting the device into a "selfish" one. In this project, we follow a radically distributed approach, in which all networking functions are embedded in the terminals themselves. Because they act as network nodes and terminals at the same time, we call these devices *terminal nodes*. A network of terminal nodes is an autonomous, self-organized network, completely independent of any fixed infrastructure or other equipment. Our solution is based on the application of a tamper resistant security module in each device and cryptographic protection of messages.

The Packet Trade Model (PTM):

In this approach, the packet does not carry nuggets, but it is traded for nuggets by intermediate terminodes. Each intermediary "buys" it from the previous one for some nuggets4, and "sells" it to the next one (or to the destination) for more nuggets. In this way, each intermediary that provided a service by forwarding the packet, increases its number of nuggets, and the total cost of forwarding the packet is covered by the destination of the packet.

The Packet Purse Model (PPM)

In this model, the originator of the packet pays for the packet forwarding service. The service charge is distributed among the forwarding terminodes in the following way: When sending the packet, the originator loads it with a number of nuggets sufficient to reach the destination. Each forwarding terminode acquires one or several nuggets from the packet and thus, increases the stock of its nuggets; the number of nuggets depends on the direct connection on which the packet is forwarded (long distance requires more nuggets). If a packet does not have enough nuggets to be forwarded, then it is discarded.

2. Fair allocation of resources is an important consideration in the design of wireless networks. In this paper, we consider the setting of multihop wireless networks with multiple routing paths and develop an online flow control and scheduling algorithm for packet admission and link activation that achieves high aggregate throughput while providing different data flows with a fair share of network capacity. For fairness provisioning, we seek to maximize the minimum throughput provided to flows in the network. To cope with different degrees of data reliability among the different links in the network, we use different channel code rates as appropriate. While we expect performance improvement using channel coding and multipath routing, the main contribution of our work is a joint treatment of network stability, multipath routing and link-level reliability in meeting the overarching goal of maxmin fairness. We develop a decentralized, and hence practical, scheduling policy that addresses various concerns and demonstrate via simulations, that it is competitive with respect to an optimal centralized rate allocator. We also evaluate the fairness provisioning under the proposed algorithm and show that channel coding improves the performance of the network significantly. Finally, we show through simulations that the proposed algorithm outperforms a class of existing approaches on fairness provisioning, which are developed based on utility maximization.

Channel coding:

Channel coding has been used to tolerate link-level errors by adding redundant bits to the data bits in a codeword. By increasing the number of redundant bits in a codeword, one can increase the probability of decoding a codeword correctly at the receiver; the tradeoff is that redundancy increases the network load thereby reducing the effective data throughput.

The aspect of improving the reliability of data delivery through channel coding in a wireless network has been considered. Lee *et al.* have examined the rate-reliability tradeoff, but they considered a single routing path between each source-destination pair. In previous work, we improved the network throughput with channel coding and multipath routing. Maxmin fairness provisioning is also considered in that context. The impact of channel coding and multipath routing on delay improvement is also studied. However, we used a centralized NUM approach to determine the average rates but not the exact scheduling policy.

Multipath routing:

Multipath routing has been explored to improve network behavior. It considered networks with multipath routing and channel coding. We proved the convergence of the

algorithm analytically. Through simulations, we showed that the proposed algorithm followed the optimal centralized approach with under control degree of sub-optimality. We also showed that the proposed algorithm improves the performance of the network regarding fairness comparing to the other approaches which ignore fairness provisioning.

3. The employment of adequate trust methods in mobile ad hoc networks (MANET) has been receiving increasing attention during the last few years, and several trust and security establishment solutions that rely on cryptographic and hashing schemes have been proposed. These schemes, although effective, produce significant processing and communication overheads and consume energy, and, hence, they do not take into account the idiosyncrasies of a MANET. More recently, cooperation enforcement methods have been proposed for trust establishment in MANET. These schemes, classified as reputation-based and credit-based, are considered suitable for ad hoc networks, where key or certificate distribution centers are absent or ephemerally present, and for networks that consist of devices with limited processing, battery, and memory resources. Cooperation enforcement methods do not provide strong authentication of entities. Instead, they contribute to the identification of the trustworthiness of peers and to the enforcement cooperation using mutual incentives. This paper surveys the most important cooperation enforcement methods that have been introduced, providing a comprehensive comparison between the different proposed schemes.

REPUTATION BASED MODELS

Confidant

It employs four functional components relying on each node, which include: (a) a monitor, (b) reputation records for first-hand and trusted second-hand observations about routing and forwarding function of other nodes, (c) trust records to control the trust that is given to received warnings, and, (d) a path manager to take routing decisions that avoid malicious nodes.

CORE

This scheme, introduced by Michiardi and Molva, relies on the DSR routing protocol. It stimulates node collaboration through monitoring of the cooperativeness of nodes and a reputation mechanism. It uses first and second-hand experiences, combined by a specialized function. This function is used by the Watchdog mechanism for the evaluation of other nodes' behavior.

SORI

It combines features of the fist-hand schemes and those that use reputation spreading. In SORI the nodes exchange reputation information only with their neighbors. This way a no-cooperative node will be punished by all of its neighbors (who share the reputation information about its misbehavior), instead of just the ones who are directly affected by this node.

OCEAN

It relies only on first-hand observations. Every node maintains ratings for each neighboring node and monitors their behaviors through promiscuous observations. Positive or negative events are recorded through the reaction of a neighbor that is expected to forward a packet. Rating is initialized to a neutral value.

CREDIT-BASED MODELS

Sprite

The simple, cheat-proof, credit-based system for mobile ah-hoc networks was proposed. It does not require tamper-proof hardware to prevent the deviation of payment units, but incorporates a centralized credit clearance service (CCS). When receiving a packet, a node keeps the signed receipt of this packet, which was generated by the source node. Sprite assumes that each node has a public key certificate published by a CA.

Token-Based Cooperation Enforcement

This scheme, introduced, protects both routing and packet forwarding in the context of the AODV protocol. It is self-organized, without assuming any a-priori trust between the nodes, or the existence of any centralized trust entity.

Ad hoc-VCG

Energy-efficiency is a parameter of high importance for the MANET routing protocols. It ensures that a packet gets routed along the most energy-efficient path. The total energy of a routing path is the sum on the emission energy levels used at the source and at each intermediate node.

4. Security in mobile ad hoc networks is hard to achieve due to dynamically changing topology and fully decentralized characteristics as well as vulnerability and scarcity of wireless links. Wired equivalent security is difficult to provide in ad hoc networks due to high dynamics, wireless link vulnerability, and requirement of complete decentralization. Especially mutual authentication among nodes in a self-organized mode of ad hoc network, where a single

definition of trust is hard to build, is very difficult. This leads to several loopholes in previously established security architectures and intrusion detection systems if employed to ad hoc networks. Also, typical to ad hoc routing major security lacks are unfair participation of nodes in the system, and frequent attacks to the routing protocols by ad hoc nodes that do not want to forward foreign packets but use other nodes to forward their own packets. Contrary to detection based approaches to tackle this situation, we propose a motivation based approach which does not require mutual authentication. We enable this by providing a) a realistic architecture of ad hoc access network to an ISP, b) a workable business model for charging in this architecture and c) necessary security protocol to implement the charging scheme. We propose for the latter a protocol specification and give a formal validation. It is also suggested that in a co-operative network, detection can help in revealing the selfish node's identity to the community rating system, which enables the system to punish the selfish nodes

Charging Policy

The motivation behind the charging scheme is ISP operator's interest in promoting his subscriber to form an ad hoc network. The benefits are two fold for the operator: saving resource at the access point, as well as earning money from its subscriber communication without spending his own resource for the same. Other technical gain could be better throughput for communicating users during heavy load situation at *AP* or unavailability of *AP*. Our charging scheme for an ad hoc stub network is based on usage-, or more precisely volume-based fees and credits. Assuming *MN* and *CN* both residing in the ad hoc network and given a price per unit for sending or receiving traffic ($p+$), and a negative price (reward) per unit for forwarding traffic ($p-$), it is profitable for the ISP

Apart from the fact that presence of ISP at the policy level is an enabler for ad hoc networking, need of intermittent access to Internet by ad hoc nodes, justifies the presence of ISP in the architecture level. To this end, we observe that there is another scenario of communication (centralized mode) where *AP* is involved in the communication path and *CN* either resides in a different ad hoc network or anywhere in the backbone.

5. Advances in mobile communication theory have enabled the development of different wireless access technologies. Alongside the revolutionary progress in wireless access technologies, advances in wireless access devices such as laptops, palmtops, and cell phones and mobile middleware have paved the way for the delivery of beyond-voice-type services while on the

move. This sets the platform for high-speed mobile communications that provide high-speed data and both real and non-real time multimedia to mobile users. Today's wireless world uses several communication infrastructures such as Bluetooth for personal area, IEEE 802.11 for local area, Universal Mobile Telecommunication System (UMTS) for wide area, and Satellite networks for global networking other hand, since these wireless networks are complementary to each other, their integration and coordinated operation can provide ubiquitous “always best connection" quality mobile communications to the users. This paper discusses the different architectures of wireless networks and the different factors to be considered while designing a hybrid wireless network. The different factors to be considered for design of a hybrid wireless network and the different networks have been explored in this paper.

Multihop relaying

In which massages are sent from the source to destination by relaying through the intermediate hopes. Routing is done through intermediate nodes and\or base stations. Base stations are used for keeping routing information. Multihop relaying is used in this architecture. It is self-organized network. Every node looks for activities of its neighbour. Nodes exchange topology information periodically. It tries to find new paths on path breaks through routing protocols. These architectures can be divided on the basis of system with dedicated relay stations or on the systems host-cum relay stations. The next generation networks are expected to reuse the spectrum better. If we want to increase the throughput of traditional cellular networks, we use multi hop cellular network (MCN), integrated cellular and ad hoc relaying system (ICAR), hybrid wireless network (HWN) architecture, self organizing packet radio networks with overlay (SOPRANO), multi power architecture for cellular network (MuPAC) & throughput enhanced wireless in local loop (TwiLL). Examples of other hybrid architecture include mobile assisted data forwarding (MADF) system, ad hoc GSM (A-GSM), directional throughput enhanced wireless in local loop (DwiLL) and unified cellular and ad hoc network (UCAN).

PREPOSED SYSTEM:

In order to efficiently and securely charge the source and destination nodes, the lightweight hashing operations are used in the ACK packets to reduce the number of public-key-cryptography operations. The destination node generates a hash chain and signs its root, and acknowledges message reception by releasing a hash value from the hash chain. In this way, the destination node generates a signature per group of messages instead of generating a signature

per message. Furthermore, instead of generating a check per message or generating a nodal check for each intermediate node, a small-size check containing the payment data for all the intermediate nodes is generated per route. In addition, trusting one node to submit the check is not secure because this node may collude with the source and destination nodes to not submit the check. Instead of submitting the checks by all the intermediate nodes to thwart collusion attack, a Probabilistic- Check-Submission scheme is proposed to reduce the number of submitted checks and protect against collusion attack. If each intermediate node submits a low ratio of randomly chosen checks, most of the checks can be probabilistically submitted under collusion attack. Extensive analysis and simulations demonstrate that FESCIM can secure the payment, charge the source and destination nodes almost computationally free and significantly reduce the number of generated and submitted checks.

Advantage

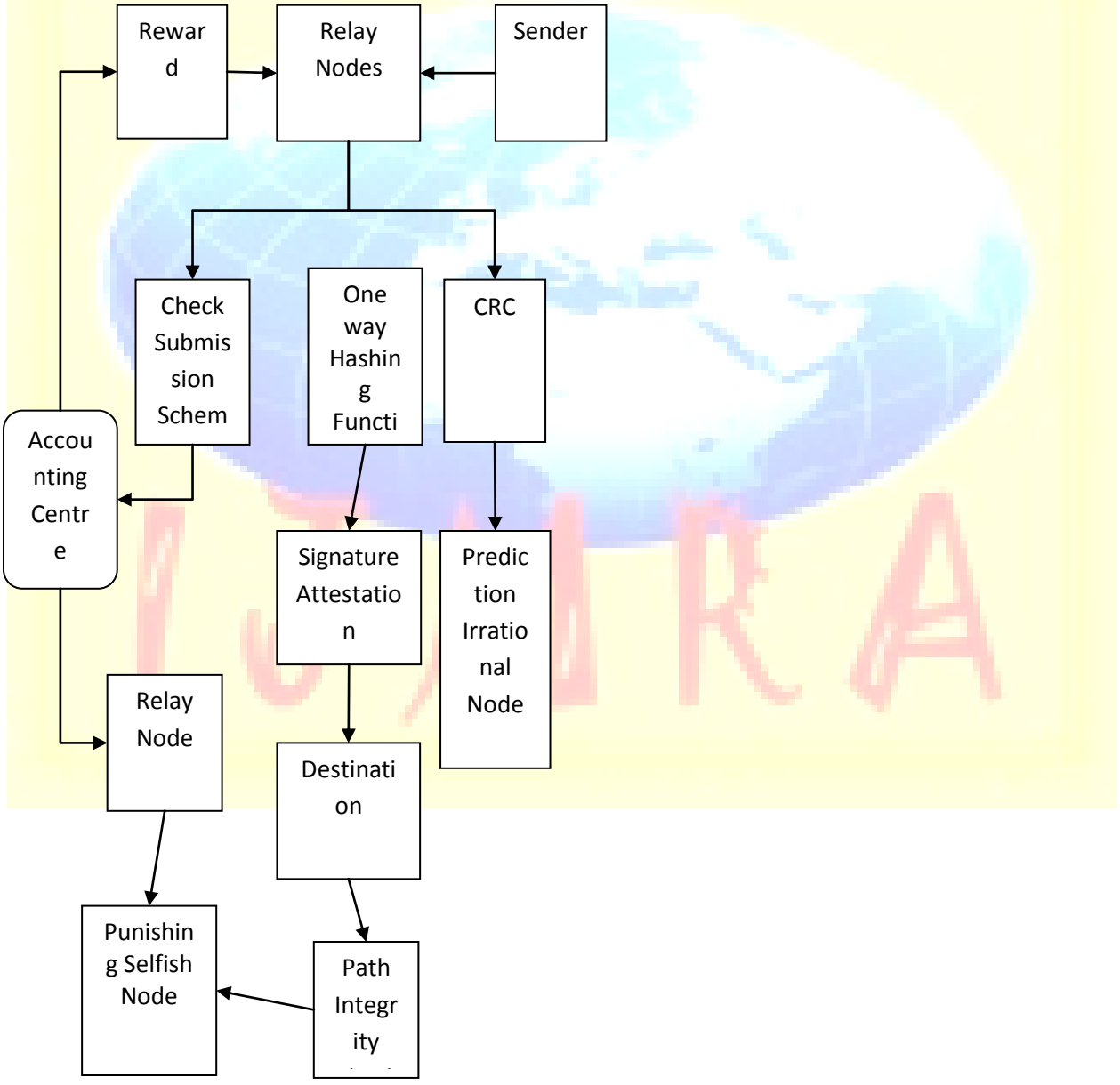
- Probabilistic-Check-Submission scheme has been proposed to reduce the number of submitted checks and protect against the collusion attack.
- It significantly reduces the overhead of storing, submitting, and processing the checks.

Relationship between the existing system and proposed system

In existing system, if the intermediate nodes are rewarded for relaying the messages that do not reach the destination node, the colluding nodes can drop a message and relay only the source node's signature that is much shorter than the message to claim the payment for relaying the message and also a check per message or generating a nodal check for each intermediate node is generated in each time. In order to avoid this overhead, a small-size check containing the payment data for all the intermediate nodes is generated per route. Therefore, this Probabilistic-Check-Submission scheme is proposed to reduce the number of submitted checks and protect against collusion attack. To securely implement the charging policy in existing system, two signatures are usually required per message (one from the source node and the other from the destination node) to prevent payment repudiation and manipulation. Nevertheless, the extensive use of the public key cryptography is very costly, which degrades the network performance and stimulates the nodes to behave selfishly. So the proposed system has replaced the destination node's signature with the lightweight hashing operations are used to reduce the number of public-key-cryptography operations. Since a trusted party may not be involved in the

communication sessions, the nodes usually compose undeniable proof of packet relaying called check, and submit the checks to a central unit called the accounting center (AC) for clearance. Therefore, instead of generating a signature per ACK packet, one signature is generated per Z ACKs. Each intermediate node verifies the hash value. In the existing system, there are two signatures per packet is generated one from the source and the other from the destination, this proposed system replaced the destination node's signature with hashing operations to reduce the number of public-key-cryptography operations nearly by half.

ARCHITECTURE DIAGRAM:



Advantages

- The source and destination nodes can communicate freely.
- The unused resource of selfish node can be utilized to transmit the data instead of accessing the resource from outside zone.
- Without handling the difficulties that generic multi hop routing cause, the two-hop-relay scheme retains low system complexity while significantly improving system performance.

ALGORITHM USED & EVALUATION

One-way hashing is used to generate a digital fingerprint of data. Such fingerprints are commonly used in digital signatures. For instance, if you electronically sign a contract, part of the signature affixed to the document includes a fingerprint of what you signed. This way someone cannot change the terms of the contract after the fact. Likewise, your digital signature cannot be lifted from one document and affixed to another, different document. The ``fingerprint'' generated is a hash value. One-way hashing functions take input streams, called **pre-text**, and map them to hash values. A hashing algorithm, $H$, is ``one-way'' if it is computationally difficult to arrive at x such that $H(x) = h$. That is, if you have a known hash value you cannot reverse the process of computation and arrive at a document that has that hash value.One of the challenges involved with creating one-way hash functions is that they must operate on input data streams of variable size. It should be possible to obtain a digital fingerprint of short and long input messages alike. In most traditional hashing systems input data is of a fixed length.A common way for one-way hash functions to deal with the variable length input problem is called a **compression function**.

1. **ROUTE DISCOVERY PHASE**

The route discovery phase is to establish an end-to-end route, the source node broadcasts the Route Request Packet (RREQ) containing the identities of the source (IDS) and the destination (IDD) nodes where the destination node will send the Acknowledgement to the source from that message the route will be discovered and maintained that route for communication till all packets get transmitted.

2. DATA GENERATION AND RELAY PHASE

In data generation phase the project will implement how the data will be transferred to the destination by appending the signed signature which will be generated by each co-operative node and forward the signature generated by T-Hash Function as an ACK. After receiving the ACK of the last message, the source node sends End of Session (EoS) packet to close the session.

3. COMMUNICATION MODEL

The communication model includes the submission of bill generated by each node to claim their amount of energy utilized to transmit the data to the destination. The bill will be collected by the border node and generated in the form of check (Digital signature) and submitted it to the AC(Accounting Center). This module involves in monitoring process like verifying the check and whether the incentive and reward has been reached to the co-operative node.

4. REWARD COLLECTION

In this phase the reimbursement of energy will take place to each and every co-operative node with reward. This process is enhanced under the control of AC.

5. CRC MONITORING

This module is implemented for monitoring purpose as well as for error checking process. The CRC will generate a Parity bit which will be appended to each packet; the status of each node will be gathered from the parity bit appended in the packet.

CONCLUSION

This project proposes FESCIM, a Fair, Efficient, and Secure Cooperation Incentive Mechanism, to stimulate the node cooperation in MCN. In order to efficiently and securely charge the source and destination nodes, the lightweight hashing operations are used in the ACK packets to reduce the number of public-key-cryptography operations. Reducing the overhead of the payment checks is essential for the efficient implementation of the incentive mechanism due to the large number of payment transactions. Instead of generating a check per message, a small-size check can be generated per route, and a check submission scheme is proposed to reduce the number of submitted checks and protect against collusion attacks. Extensive analysis and simulations demonstrate that our mechanism can secure the payment and significantly reduce the checks' overhead, and the fair charging policy can be implemented almost computationally free by using hashing operation.

FUTURE ENHANCEMENT

In order to eliminate the huge overhead of path construction and maintenance, it is going to use a symmetric cryptographic algorithm to replace the asymmetric one so as to reduce the cryptographic overhead. They design a light weight mutual anonymous P2P protocol, Rumor Riding (RR), in which anonymous paths are automatically constructed via the rumors' random walks. So they can reduce the memory management cost for initiator.

REFERENCES:

1.3rd Generation Partnership Project, Technical Specification GroupRadio Access Network, "Opportunity Driven Multiple Access,"3G Technical Report 25.924, Version 1.0.0, Dec. 1999.

2.S. Marti, T. Giuli, K. Lai, and M. Baker, "Mitigating RoutingMisbehavior in Mobile Ad Hoc Networks," Proc. ACM MobiCom,pp. 255-265, Aug. 2000.

3.P. Michiardi and R. Molva, "Simulation-Based Analysis ofSecurity Exposures in Mobile Ad Hoc Networks," Proc. EuropeanWireless Conf., Feb. 2002.

4.J. Hu, "Cooperation in Mobile Ad Hoc Networks," TechnicalReport TR-050111, Computer Science Dept., Florida State Univ.,Jan. 2005.

5.G. Marias, P. Georgiadis, D. Flitzanis, and K. Mandalas,"Cooperation Enforcement Schemes for MANETs: A Survey,"J. Wireless Comm. and Mobile Computing, vol. 6, no. 3, pp. 319-332,2006.

6.C. Song and Q. Zhang, "OMH-Suppressing Selfish Behavior inAd Hoc Networks with One More Hop," Mobile Networks andApplications, vol. 14, no. 2, pp. 178-187, Feb. 2009.

7.D. Djenouri and N. Badache, "On Eliminating Packet Droppers inMANET: A Modular Solution," Ad Hoc Networks, vol. 7, no. 6,pp. 1243-1258, Aug. 2009.

8.N. Salem, L. Buttyan, J. Hubaux, and M. Jakobsson, "NodeCooperation in Hybrid Ad Hoc Networks," IEEE Trans. MobileComputing, vol. 5, no. 4, pp. 365-376, Apr. 2006.

9.S. Zhong, J. Chen, and R. Yang, "Sprite: A Simple, Cheat-Proof,Credit Based System for Mobile Ad-Hoc Networks," Proc. IEEEINFOCOM, vol. 3, pp. 1987-1997, Mar./Apr. 2003.

10.H. Janzadeh, K. Fayazbakhsh, M. Dehghan, and M. Fallah, "ASecure Credit-Based Cooperation Stimulating Mechanism forMANETs Using Hash Chains," Future Generation ComputerSystems, vol. 25, no. 8, pp. 926-934, Sept. 2009.

11.B. Lamparter, K. Paul, and D. Westhoff, "Charging Support forAd Hoc Stub Networks," J. Computer Comm., vol. 26, no. 13,pp. 1504-1514, 2003.

12.S. Miner and J. Staddon, "Graph-Based Authentication of DigitalStreams," Proc. IEEE Symp. Security and Privacy, pp. 232-246, May2001.

13.D. Johnson and D. Maltz, "Dynamic Source Routing in Ad HocWireless Networks," Mobile Computing, pp. 153-181, chapter 5,Kluwer Academic, 1996.

14.A. Weyland and T. Braun, "Cooperation and Accounting Strategyfor Multi-Hop Cellular Networks," Proc. IEEE Local and MetropolitanArea Networks (LANMAN '04), pp. 193-198, Apr. 2004.

15.A. Weyland, "Cooperation and Accounting in Multi-Hop CellularNetworks," PhD thesis, Univ. of Bern, Nov. 2005.

16.J. Hubaux, L. Buttya´n, and S. Capkun, "The Quest for Security inMobile Ad Hoc Networks," Proc. ACM Symp. Mobile Ad HocNetworking and Computing, Oct. 2001.